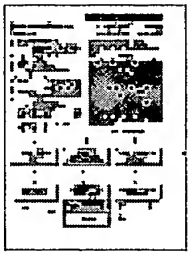
The Delphion Integrated View

Title: **JP11168461A2: METHOD AND EQUIPMENT FOR COMMUNICATING INFORMATION**

Derwent Title: Information communication method between IC card and IC card terminal - involves authenticating IC card when information obtained by synthesizing random number transmitted from IC card terminal to IC card matches with that transmitted from IC card and card terminal [Derwent Record]



Country: **JP** Japan
Kind: **A**

Inventor: **OTA MICHIHIRO**;

Assignee: **NIPPON CONLUX CO LTD**
News, Profiles, Stocks and More about this company

Published / Filed: **1999-06-22** / 1997-12-04

Application Number: **JP1997000334254**

IPC Code: Advanced: **G06K 17/00**; **G09C 1/00**; **H04L 9/32**;
Core: more...
IPC-7: **G06K 17/00**; G09C 1/00; H04L 9/32;

Priority Number: 1997-12-04 **JP1997000334254**

Abstract:

PROBLEM TO BE SOLVED: To provide a method and equipment for communicating information with which a cryptographic key is prevented from being decoded in simple configuration, illegal action based on forgery after authentication is prevented as well and communication is enabled not only between an IC card and an IC card terminal but also between IC cards.

SOLUTION: An IC card terminal 1 and an IC card 2 communicate information by performing enciphering processing, the IC card terminal 1 compares a random number synthesized with the information received from the IC card 2 with a random number synthesized with the information transmitted from the IC card terminal 1 to the IC card 2 in advance through a comparison means 14. Only when both the random numbers are equal, the processing of received information is permitted to a data processing means 15 by authenticating the IC card. The IC card 2 similarly processes the received information after the IC card terminal 1 is authenticated as well.

Family: None

Other Abstract Info: None

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-168461
(43)Date of publication of application : 22.06.1999

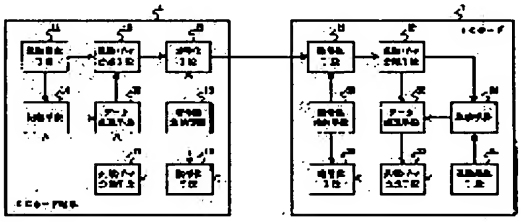
(51)Int.Cl. H04L 9/32
G06K 17/00
G09C 1/00
G09C 1/00

(21)Application number : 09-334254
(22)Date of filing : 04.12.1997

(71)Applicant : NIPPON CONLUX CO LTD
(72)Inventor : OTA MICHIHIRO

(54) METHOD AND EQUIPMENT FOR COMMUNICATING INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and equipment for communicating information with which a cryptographic key is prevented from being decoded in simple configuration, illegal action based on forgery after authentication is prevented as well and communication is enabled not only between an IC card and an IC card terminal but also between IC cards.
SOLUTION: An IC card terminal 1 and an IC card 2 communicate information by performing enciphering processing, the IC card terminal 1 compares a random number synthesized with the information received from the IC card 2 with a random number synthesized with the information transmitted from the IC card terminal 1 to the IC card 2 in advance through a comparison means 14. Only when both the random numbers are equal, the processing of received information is permitted to a data processing means 15 by authenticating the IC card. The IC card 2 similarly processes the received information after the IC card terminal 1 is authenticated as well.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1] In the information correspondence procedure which communicates by repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment In case the 1st information over said 2nd equipment is transmitted from said 1st equipment, while generating the 1st random number with said 1st equipment Compound the 1st generated this random number and this 1st information, and it considers as the 1st synthetic information. this -- said 2nd equipment which enciphered the 1st synthetic information, transmitted to said 2nd equipment as 1st encryption information, and received said 1st encryption information from said 1st equipment It separates into said the 1st information and said 1st random number, after decrypting the 1st this encryption information which received. In case processing to said 1st information is performed and the 2nd information over said 1st equipment is transmitted from said 2nd equipment, while generating the 2nd random number with said 2nd equipment Compound the 2nd generated this random number, this 2nd information, and said 1st separated random number, and it considers as the 2nd synthetic information. this -- said 1st equipment which enciphered the 2nd synthetic information, transmitted to said 1st equipment as 2nd encryption information, and received the 2nd encryption information from said 2nd equipment It separates into said the 2nd information, said 2nd random number, and said 1st random number, after decrypting the 2nd this encryption information which received. When the 1st separated this random number is compared with said 1st generated random number and said 1st separated random number and said 1st generated random number are in agreement with this comparison, attest said 2nd equipment and processing to said 2nd information is performed. In case the 3rd information over said 2nd equipment is transmitted from said 1st equipment, while generating the 3rd random number with said 1st equipment Compound the 3rd generated this random number, this 3rd information, and said 2nd separated random number, and it considers as the 3rd synthetic information. this -- said 2nd equipment which enciphered the 3rd synthetic information, transmitted to said 2nd equipment as 3rd encryption information, and received the 3rd encryption information from said 1st equipment It separates into said the 3rd information, said 3rd random number, and said 2nd random number, after decrypting the 3rd this encryption information which received. When the 2nd separated this random number is compared with said 2nd generated random number and said 2nd separated random number and said 2nd generated random number are in agreement with this comparison, attest said 1st equipment and processing to said 3rd information is performed. The information correspondence procedure characterized by repeating the above-mentioned processing until transmission and reception of the information between said 1st equipment and said 2nd equipment are completed.
[Claim 2] The encryption and the decryption which said 1st equipment performs, the encryption which said 2nd equipment performs, and a decryption are an information correspondence procedure according to claim 1 characterized by being carried out using the same cryptographic key.
[Claim 3] It is the information correspondence procedure according to claim 1 characterized by being the IC card terminal with which said 1st equipment is an IC card, and said 2nd equipment performs the communication link of said IC card and information.
[Claim 4] Said the 1st equipment and said 2nd equipment are an information correspondence procedure according to claim 1 characterized by being an IC card.
[Claim 5] In the information correspondence procedure which communicates by repeating informational

transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment In case the 1st information over said 2nd equipment is transmitted from said 1st equipment, while generating the 1st random number with said 1st equipment Compound the 1st encryption information and said 1st generated random number, and it transmits to said 2nd equipment as the 1st transmit information. this 1st information -- enciphering -- the 1st encryption information -- carrying out -- this -- Said 2nd equipment which received said 1st transmit information from said 1st equipment After dividing the 1st this transmit information which received into said 1st random number and said 1st encryption information, this, while generating the 2nd random number with said 2nd equipment, in case the 1st encryption information is decrypted to said 1st information, processing to this 1st information is performed and the 2nd information over said 1st equipment is transmitted from said 2nd equipment Compound this 2nd information and said 1st separated random number, and it considers as the 2nd synthetic information. Compound the 2nd encryption information and said 2nd generated random number, and it transmits to said 1st equipment as the 2nd transmit information. this -- the 2nd synthetic information -- enciphering -- the 2nd encryption information -- carrying out -- this -- Said 1st equipment which received the 2nd transmit information from said 2nd equipment After dividing the 2nd this transmit information which received into said 2nd random number and said 2nd encryption information, Decrypt the 2nd encryption information to said 2nd synthetic information, and the 2nd this decrypted synthetic information is divided into said the 1st random number and said 2nd information. this -- When the 1st separated this random number is compared with said 1st generated random number and said 1st separated random number and said 1st generated random number are in agreement with this comparison, attest said 2nd equipment and processing to said 2nd information is performed. In case the 3rd information over said 2nd equipment is transmitted from said 1st equipment, while generating the 3rd random number with said 1st equipment Compound this 3rd information and said 2nd separated random number, and it considers as the 3rd synthetic information. Compound the 3rd encryption information and said 3rd generated random number, and it transmits to said 2nd equipment as the 3rd transmit information. this -- the 3rd synthetic information -- enciphering -- the 3rd encryption information -- carrying out -- this -- Said 2nd equipment which received the 3rd transmit information from said 1st equipment After dividing the 3rd this transmit information which received into said 3rd random number and said 3rd encryption information, Decrypt the 3rd encryption information to said 3rd synthetic information, and the 3rd this decrypted synthetic information is divided into said the 2nd random number and said 3rd information. this -- When the 2nd separated this random number is compared with said 2nd generated random number and said 2nd separated random number and said 2nd generated random number are in agreement with this comparison, attest said 1st equipment and processing to said 3rd information is performed. The information correspondence procedure characterized by repeating the above-mentioned processing until transmission and reception of the information between said 1st equipment and said 2nd equipment are completed.

[Claim 6] The encryption and the decryption which said 1st equipment performs, the encryption which said 2nd equipment performs, and a decryption are an information correspondence procedure according to claim 5 characterized by being carried out using the same cryptographic key.

[Claim 7] It is the information correspondence procedure according to claim 5 characterized by being the IC card terminal with which said 1st equipment is an IC card, and said 2nd equipment performs the communication link of said IC card and information.

[Claim 8] Said the 1st equipment and said 2nd equipment are an information correspondence procedure according to claim 5 characterized by being an IC card.

[Claim 9] In the information communication device which communicates by repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment said 1st equipment The 1st information processing means, the 1st random-number-generation means, the 1st synthetic means, the 1st encryption means, the 1st decryption means, the 1st separation means, and the 1st comparison means are provided. Said 2nd equipment The 2nd information processing means, the 2nd random-number-generation means, the 2nd synthetic means, the 2nd encryption means, the 2nd decryption means, the 2nd separation means, and the 2nd comparison means are provided. When said 1st equipment transmits information to said 2nd equipment While outputting the information which said 1st information processing means transmits, said 1st random-number-generation means generates a random number. The random number which said 2nd

equipment contained in information just before said 1st separation means received from said 2nd equipment generated is separated and acquired. After compounding the information which said 1st information processing means outputted, the random number which said 1st random-number-generation means generated, and the random number which said 1st separation means acquired with said 1st synthetic means, When it enciphers with said 1st encryption means, it transmits as encryption information and said 2nd equipment transmits information to said 1st equipment While outputting the information which said 2nd information processing means transmits, said 2nd random-number-generation means generates a random number. The random number which said 1st equipment contained in information just before said 2nd separation means received from said 1st equipment generated is separated and acquired. After compounding the information which said 2nd information processing means outputted, the random number which said 2nd random-number-generation means generated, and the random number which said 2nd separation means acquired with said 2nd synthetic means, When it enciphers with said 2nd encryption means, it transmits as encryption information and said 1st equipment receives the encryption information from said 2nd equipment It separates into the information which said 2nd information processing means outputted with said 1st separation means, the random number which said 2nd random-number-generation means generated, and the random number which said 2nd separation means acquired, after decrypting the received this encryption information with said 1st decryption means. Said 1st comparison means compares the acquired this random number and the random number which said 1st random-number-generation means generated. The information which said 2nd information processing means separated with said 1st separation means when this comparison result was coincidence outputted is processed with said 1st information processing means. When said 2nd equipment receives the encryption information from said 1st equipment It separates into the information which said 1st information processing means outputted with said 2nd separation means, the random number which said 1st random-number-generation means generated, and the random number which said 1st separation means acquired, after decrypting the received this encryption information with said 2nd decryption means. Said 2nd comparison means compares the acquired this random number and the random number which said 2nd random-number-generation means generated. The information communication device characterized by processing the information which said 1st information processing means separated with said 2nd separation means when this comparison result was coincidence outputted with said 2nd information processing means.

[Claim 10] In transmitting information to said 2nd equipment before said 1st equipment receives information from said 2nd equipment Said 1st synthetic means compounds only the information which said 1st information processing means outputted, and the random number which said 1st random-number-generation means generated. In transmitting information to said 1st equipment before said 2nd equipment receives information from said 1st equipment Said 2nd synthetic means compounds only the information which said 2nd information processing means outputted, and the random number which said 2nd random-number-generation means generated. When information is received from said 2nd equipment before said 1st equipment transmitted information to said 2nd equipment The information which said 2nd information processing means separated with said 1st separation means, without said 1st comparison means comparing a random number outputted is processed with said 1st information processing means. When information is received from said 1st equipment before said 2nd equipment transmitted information to said 1st equipment The information communication device according to claim 9 characterized by processing the information which said 1st information processing means separated with said 2nd separation means, without said 2nd comparison means comparing a random number outputted with said 2nd information processing means.

[Claim 11] Said 1st encryption means, said 2nd encryption means, said 1st decryption means, and said 2nd decryption means are an information communication device according to claim 9 or 10 characterized by using the same cryptographic key.

[Claim 12] It is the information communication device according to claim 9 or 10 characterized by being the IC card terminal with which said 1st equipment is an IC card, and said 2nd equipment performs the communication link of said IC card and information.

[Claim 13] Said the 1st equipment and said 2nd equipment are an information communication device according to claim 9 or 10 characterized by being an IC card.

[Claim 14] In the information communication device which communicates by repeating informational

transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment said 1st equipment The 1st information processing means, the 1st random-number-generation means, the 1st upper composition means, the 1st lower layer composition means, the 1st encryption means, the 1st decryption means, the 1st upper separation means, the 1st lower layer separation means, and the 1st comparison means are provided. Said 2nd equipment possesses the 2nd information processing means, the 2nd random-number-generation means, the 2nd upper composition means, the 2nd lower layer composition means, the 2nd encryption means, the 2nd decryption means, the 2nd upper separation means, the 2nd lower layer separation means, and the 2nd comparison means. When said 1st equipment transmits information to said 2nd equipment While outputting the information which said 1st information processing means transmits, said 1st random-number-generation means generates a random number. The random number which said 2nd equipment contained in information just before said 1st separation means received from said 2nd equipment generated is separated and acquired. After compounding the information which said 1st information processing means outputted, and the random number which said 1st separation means acquired with said 1st lower layer composition means, Encipher with said 1st encryption means, consider as encryption information, and it transmits as synthetic information which compounded this encryption information and the random number which said 1st random-number-generation means generated with said 1st upper composition means. When said 2nd equipment transmits information to said 1st equipment While outputting the information which said 2nd information processing means transmits, said 2nd random-number-generation means generates a random number. The random number which said 1st equipment contained in information just before said 2nd separation means received from said 1st equipment generated is separated and acquired. After compounding the information which said 2nd information processing means outputted, and the random number which said 2nd separation means acquired with said 2nd lower layer composition means, Encipher with said 2nd encryption means, consider as encryption information, and it transmits as synthetic information which compounded this encryption information and the random number which said 2nd random-number-generation means generated with said 2nd upper composition means. When said 1st equipment receives the synthetic information from said 2nd equipment After said 1st upper separation means separates the random number which said 2nd random-number-generation means generated from the received this synthetic information, It separates into the information which decrypted with said 1st decryption means and said 2nd information processing means outputted with said 1st separation means further, and the random number which said 2nd separation means acquired. Said 1st comparison means compares the acquired this random number and the random number which said 1st random-number-generation means generated. The information which said 2nd information processing means separated with said 1st separation means when this comparison result was coincidence outputted is processed with said 1st information processing means. When said 2nd equipment receives the synthetic information from said 1st equipment After said 2nd upper separation means separates the random number which said 1st random-number-generation means generated from the received this synthetic information, It separates into the information which decrypted with said 2nd decryption means and said 1st information processing means outputted with said 2nd separation means further, and the random number which said 1st separation means acquired. Said 2nd comparison means compares the acquired this random number and the random number which said 2nd random-number-generation means generated. The information communication device characterized by processing the information which said 1st information processing means separated with said 2nd separation means when this comparison result was coincidence outputted with said 2nd information processing means.

[Claim 15] In transmitting information to said 2nd equipment before said 1st equipment receives information from said 2nd equipment Said 1st encryption means enciphers only the information which said 1st information processing means outputted. In transmitting information to said 1st equipment before said 2nd equipment receives information from said 1st equipment Said 2nd encryption means enciphers only the information which said 2nd information processing means outputted. When information is received from said 2nd equipment before said 1st equipment transmitted information to said 2nd equipment The information which said 2nd information processing means separated with said 1st separation means, without said 1st comparison means comparing a random number outputted is processed with said 1st information processing means. When information is received from said 1st

equipment before said 2nd equipment transmitted information to said 1st equipment The information communication device according to claim 14 characterized by processing the information which said 1st information processing means separated with said 2nd separation means, without said 2nd comparison means comparing a random number outputted with said 2nd information processing means.

[Claim 16] Said 1st encryption means, said 2nd encryption means, said 1st decryption means, and said 2nd decryption means are an information communication device according to claim 14 or 15 characterized by using the same cryptographic key.

[Claim 17] It is the information communication device according to claim 14 or 15 characterized by being the IC card terminal with which said 1st equipment is an IC card, and said 2nd equipment performs the communication link of said IC card and information.

[Claim 18] Said the 1st equipment and said 2nd equipment are an information communication device according to claim 14 or 15 characterized by being an IC card.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] About an information correspondence procedure and equipment, especially this invention relates to the information correspondence procedure and equipment which can communicate between an IC card and an IC card terminal and between IC cards while preventing leakage of a cryptographic key.
[0002]
[Description of the Prior Art] As compared with a magnetic card, the informational storage capacity of the IC card which carried IC (integrated circuit: integrated circuit) is large, and since it is possible to also make an operation etc. process inside an IC card, the application is various.
[0003] In the case where money information and extra sensitive information are treated depending on this application, for example, the adoption of an information correspondence procedure with high safeties, such as authentication and informational encryption, or equipment including an IC card and its peripheral device serves as important requirements.
[0004] Here, the conventional information correspondence procedure in an IC card and its peripheral device and an example of equipment are explained.
[0005] Drawing 4 is drawing having shown the flow of the block diagram having shown an example of the conventional IC card system, and a signal. As for the IC card terminal 101, the conventional IC card system possesses the confidential information storing means (KEY2) 119, the processing means 115, the encryption means (EK2) 113, and a decryption means (DK1), as shown in drawing 4 (a), and IC card 102 possesses the confidential information storing means (KEY1) 129, the comparison means 124, the processing means 125, the encryption means (EK1) 123, and the decryption means (DK2) 128, and is constituted.
[0006] Actuation in case the IC card terminal 101 performs the writing and read-out of information to IC card 102 here is explained.
[0007] If IC card 102 is inserted in the IC card terminal 101, the confidential information (KEY2) by which the IC card terminal 101 is stored in the confidential information storing means (KEY2) 119 will be transmitted to IC card 102 (step 151). IC card 102 will perform comparison collating for the confidential information (KEY1) stored in this and the confidential information storing means (KEY1) 129 with the comparison means 124, if confidential information (KEY2) is received. If confidential information (KEY2) is in agreement with confidential information (KEY1), IC card 102 will attest the IC card terminal 101 with it being a just IC card terminal, and will permit processing actuation to the processing means 125. Although the processing means 125 will start the communication link of the processing means 115 and data of the IC card terminal 101, an instruction, etc. if actuation is permitted In case it communicates, the data transmitted from the processing means 125 (M1, M3) It is enciphered and transmitted with the encryption means (EK1) 123 (steps 152 and 154), and the IC card terminal 101 decrypts this with the decryption means (DK1) 118, and the processing means 115 processes. Moreover, it is enciphered with the encryption means (EK2) 113 (M2, M4), and the data transmitted from the processing means 115 are transmitted (steps 153 and 155), IC card 102 decrypts this with the decryption means (DK2) 128, and the processing means 125 processes.
[0008] Although the cryptographic key which the encryption means (EK1) 123 and the decryption means

(DK1) 118 use needs to be the same and the cryptographic key which the encryption means (EK2) 113 and the decryption means (DK2) 128 use needs to be the same in order to perform such processing, four persons' cryptographic key may be the same. Moreover, the confidential information storing means (KEY2) 119 is constituted from input means, such as a personal identification number, and you may make it IC card 102 attest the user who operates the IC card terminal 101.

[0009] However, in the configuration shown in drawing 4 , it is monitoring the communication link between the IC card terminal 101 and IC card 102, and the problem of becoming it being possible to carry out the unjust acquisition of the confidential information comparatively easily, and possible to use rewriting and the forged IC card of the information on IC card 102 if confidential information is acquired arises.

[0010] Moreover, since the enciphered information is also always communicating using the same cryptographic key, possibility of decoding is high.

[0011] In order to cope with such a problem, while attesting without communicating confidential information between an IC card terminal and an IC card, the technique of preventing from decoding the enciphered information easily is proposed by JP,2-31289,A, JP,2-31290,A, JP,2-44389,A, JP,2-195378,A, etc.

[0012] The technique proposed by JP,2-31289,A The IC card terminal 201 which possesses the processing means 215, the encryption means (EK2) 213-1, the encryption means (EK4) 213-2, the decryption means (DK1) 218-1, and the decryption means (DK3) 218-2 as shown in drawing 5 (a), It consists of IC cards 202 possessing the processing means 225, the random-number-generation means (R) 221, the comparison means 224, the encryption means (EK1) 223-1, the encryption means (EK3) 223-2, the decryption means (DK2) 228-1, and the decryption means (DK4) 228-2.

[0013] This IC card system delivers and receives a signal by flow as shown in drawing 5 (b). First, in order that IC card 202 may attest the IC card terminal 201 Generate a random number (R) with the random-number-generation means (R) 221, encipher this with the encryption means (EK1) 223-1, and it transmits to the IC card terminal 201 (step 251). The IC card terminal 201 decrypts this with the decryption means (DK1) 218-1, enciphers the decrypted random number (R) with the encryption means (EK2) 213-1, and transmits it to IC card 202 (step 252).

[0014] an IC card -- 202 -- having received -- coding information -- a decryption -- a means (DK2) -- 228 - one -- decrypting -- this -- a decryption -- having obtained -- a random number -- (-- R --) -- random number generation -- a means -- (-- R --) -- 221 -- having generated -- a random number -- (-- R --) -- a comparison -- a means -- 224 -- comparing -- both -- being in agreement -- if -- the IC card terminal 201 -- attesting -- the processing means 225 -- authorization of operation -- giving .

[0015] This attests the IC card terminal 201 by the random number which IC card 202 generated and was transmitted having been answered by being carried out in just processing, and when the encryption means (EK1) 223-1 and the decryption means (DK1) 218-1 use the same cryptographic key and the encryption means (EK2) 213-1 and the decryption means (DK2) 228-1 are using the same cryptographic key, it is materialized. However, the cryptographic key which the encryption means (EK1) 223-1 and the encryption means (EK2) 213-1 use in this case must not be the same.

[0016] Although the processing means 225 will start the communication link of the processing means 215 and data of the IC card terminal 201, an instruction, etc. if IC card 202 attests the IC card terminal 201 and permits actuation of the processing means 225 In case it communicates, the data transmitted from the processing means 225 (M1, M3) It is enciphered and transmitted with the encryption means (EK3) 223-2 (steps 253 and 255), and the IC card terminal 201 decrypts this with the decryption means (DK3) 218-2, and the processing means 215 processes. Moreover, it is enciphered with the encryption means (EK4) 213-2 (M2, M4), and the data transmitted from the processing means 215 are transmitted (steps 254 and 256), IC card 202 decrypts this with the decryption means (DK4) 228-2, and the processing means 225 processes.

[0017] In this case, without transmitting confidential information directly unlike the system explained by drawing 4 , it is enciphering the random number used at the time of authentication by the cryptographic key, and the information acquired by wire tapping is changed each time, and it is going to make decode of a code difficult.

[0018] The technique proposed by JP,2-31290,A The IC card terminal 301 which possesses the processing means 315, the encryption means (EK2) 313-1, encryption means (ER)313-2, the decryption

means (DK1) 318-1, and decryption means (DR)318-2 as shown in drawing 6 (a), It consists of the processing means 325, the random-number-generation means (R) 321, the comparison means 324, the encryption means (EK1) 323-1, encryption means (ER)323-2, a decryption means (DK2) 328-1, and IC card 302 possessing decryption means (DR)328-2.

[0019] Although this IC card system delivers and receives a signal by flow as shown in drawing 6 (b), since the approach IC card 302 attests the IC card terminal 301 with the signal delivered and received at steps 351 and 352 is the same as that of the case where it is shown in drawing 5 , explanation is omitted.

[0020] Now, although the processing means 325 will start the communication link of the processing means 315 and data of the IC card terminal 301, an instruction, etc. if IC card 302 attests the IC card terminal 301 and actuation of the processing means 325 is permitted In case it communicates, the data transmitted from the processing means 325 (M1, M3) Encryption means (ER) By 323-2, at the time of authentication, the random number which the random-number-generation means (R) 321 generated is enciphered as a cryptographic key, and it is transmitted (steps 353 and 355), and the IC card terminal 301 decrypts this by decryption means (DR)318-2, and the processing means 315 processes. Moreover, the random number (it memorizes at the time of authentication) which the random-number-generation means (R) 321 generated in encryption means (ER)313-2 similarly at the time of authentication (M2, M4) is enciphered as a cryptographic key, the data transmitted from the processing means 315 are transmitted (steps 354 and 356), IC card 302 decrypts this by decryption means (DR)328-2, and the processing means 325 processes.

[0021] In this case, by using the random number which generated the encryption at the time of communicating data etc. at the time of authentication as a cryptographic key in addition to the system explained by drawing 5 , a cryptographic key is changed each time and it is going to make decode difficult.

[0022] Moreover, the technique proposed by JP,2-44389,A Drawing 7 As shown in (a), the processing means 415, a random-number-generation means (R2) 411, the comparison means 414, the synthetic means 412, the encryption means (EK2) 413-1, the encryption means (ER one R2) 413-2, the decryption means (DK1) 418-1, the decryption means (DK2) 418-2, and the decryption means (DR one R2) 418-3 The IC card terminal 401 to provide, The processing means 425, a random-number-generation means (R1) 421, the comparison means 424, the separation means 427, the encryption means (EK1) 423-1, the encryption means (EK3) 423-2, the encryption means (ER one R2) 423-3, the decryption means (DK2) 428-1, and the decryption means (DR one R2) 428-2 It consists of IC cards 402 to provide.

[0023] This IC card system delivers and receives a signal by flow as shown in drawing 7 (b). First, in order to attest the IC card terminal 401, IC card 402 generates a random number (R1) with the random-number-generation means (R1) 421, enciphers this with the encryption means (EK1) 423-1, and transmits it to the IC card terminal 401 (step 451). While decrypting the received encryption information with the decryption means (DK1) 418-1, in order to attest IC card 402, the IC card terminal 401 generates a random number (R2) with the random-number-generation means (R2) 411, compounds this random number (R2) and the decrypted random number (R1) with the synthetic means 412, enciphers this with the encryption means (EK2) 413-1, and transmits it to IC card 402 (step 452).

[0024] IC card 402 decrypts the coding information which received with the decryption means (DK2) 428-1, and divides it into a random number (R1) and a random number (R2) with the separation means 427 further. If it is compared by the random number (R1) and the comparison means 424 which the random-number-generation means (R1) 421 generated and both are in agreement, the separated random number (R1) will attest the IC card terminal 401, and will give authorization of operation to the processing means 425.

[0025] On the other hand, the random number (R2) separated with the separation means 427 It is enciphered with the encryption means (EK3) 423-2, and is transmitted to the IC card terminal 401. The IC card terminal 401 The comparison means 414 compares the random number (R2) which decrypted the coding information which received with the decryption means (DK3) 418-2, and was obtained by the decryption, and the random number (R2) which the random-number-generation means (R2) 411 generated. If both are in agreement, IC card 402 will be attested and authorization of operation will be given to the processing means 415.

[0026] Although the processing means 415 and the processing means 425 will start the communication

link of data, an instruction, etc. mutually if IC card 402 attests the IC card terminal 401, actuation of the processing means 425 is permitted, the IC card terminal 401 attests IC card 402 and actuation of the processing means 415 is permitted In case it communicates, the data which the processing means 425 transmits (M1, M3) With the encryption means (ER one R2) 423-3, at the time of authentication, encipher the random number (R1) which the random-number-generation means (R1) 421 generated, and the random number (R2) which the random-number-generation means (R2) 411 generated as a cryptographic key, and it is transmitted (steps 454 and 456). The IC card terminal 401 decrypts this with the decryption means (DR one R2) 418-3, and the processing means 415 processes. Moreover, the data transmitted from the processing means 415 (M2, M4) Similarly, with the encryption means (ER one R2) 413-2, at the time of authentication, encipher the random number (R1) which the random-number-generation means (R1) 421 generated, and the random number (R2) which the random-number-generation means (R2) 411 generated as a cryptographic key, and it is transmitted (steps 455 and 457). IC card 402 decrypts this with the decryption means (DR one R2) 428-2, and the processing means 425 processes.

[0027] As compared with the system which explained this system by drawing 6 , it differs in an IC card not only attests an IC card terminal, but that the IC card terminal has attested the IC card.

[0028] The technique proposed by JP,2-195378,A Drawing 8 As shown in (a), the processing means 515, a random-number-generation means (R2) 511, the encryption means (EK2) 513-1, the encryption means (ER2) 513-2, the decryption means (DK1) 518-1, the decryption means (DR2) 518-2, a register 531-1,531-2, and the EXCLUSIVE-OR-operation means 532-1,532-2 The IC card terminal 501 to provide, The processing means 525, a random-number-generation means (R1) 521, the encryption means (EK1) 523-1, the encryption means (ER2) 523-2, the decryption means (DK2) 528-1, the decryption means (DR2) 528-2, a register 541-1,541-2, and the EXCLUSIVE-OR-operation means 542-1,542-2 It consists of IC cards 502 to provide.

[0029] Especially authentication is not performed although this IC card system delivers and receives a signal by flow as shown in drawing 8 (b).

[0030] First, in advance of the communication link of data etc., IC card 502 generates a random number (R1) with the random-number-generation means (R1) 521. While storing this in a register 541-1,541-2, encipher with the encryption means (EK1) 523-1, and it transmits to the IC card terminal 501 (step 551). The IC card terminal 501 stores in a register 531-1,531-2 the random number (R1) which decrypted and obtained this with the decryption means (DK1) 518-1. Moreover, the IC card terminal 501 generates a random number (R2) with the random-number-generation means (R2) 511, this is enciphered with the encryption means (EK2) 513-1, and it transmits to IC card 502 (step 552), and IC card 502 decrypts this with a decryption means (DK2), and obtains a random number (R2).

[0031] Thus, although the IC card terminal 501 and IC card 502 will start the communication link of data, an instruction, etc. using a random number (R1) and a random number (R2) if a random number (R1) and a random number (R2) are notified mutually In case it communicates, the data transmitted from the processing means 525 (M1, M3, M5) A random number (R2) is enciphered as a cryptographic key with the encryption means (ER2) 523-2, an exclusive OR with the random number (R1) which is the contents further stored in the register 541-1 with the EXCLUSIVE-OR-operation means 542-1 calculates, and this result of an operation is transmitted (step 553). The IC card terminal 501 performs the reverse operation of the operation in the EXCLUSIVE-OR-operation means 542-1 using the random number (R1) which is the contents in which the coding information which received is stored by the register 531-1 with the EXCLUSIVE-OR-operation means 532-1, a random number (R2) is decrypted as a cryptographic key with the decryption means (DR2) 518-2, and the processing means 515 processes this. Moreover, the contents stored in a register 531-1,541-1 are changed into the data (M1) which were the contents of a communication link after a communication link, and an exclusive OR with data (M1) calculates them by the next communication link (step 555).

[0032] Similarly, the data transmitted from the processing means 515 use a random number (R2) for a cryptographic key (M2, M4, M6), and an exclusive OR with the contents of storing of a register 531-1 calculates, and is transmitted.

[0033] Since this system serves as that the cryptographic key is changed for every communication link by the operation of an exclusive OR, and consent, decode of encryption information is difficult.

[0034]

[Problem(s) to be Solved by the Invention] However, with the technique proposed by JP,2-31289,A, since it is always communicating using the same cryptographic key after attesting, the same cipher may communicate and decode of a cryptographic key may be performed. For example, if the same cryptographic key is used to the plaintext which communicates each time [, such as an access request and an access permission,], the always same cipher will communicate. If the cryptographic key after authentication is decoded, after an IC card attests an IC card terminal, it intervenes in a communication link, and a just IC card terminal will be impersonated and unjust access to an IC card will be attained. Moreover, since the configuration or signal processing of an IC card and an IC card terminal are not the same, it cannot communicate between IC cards, without minding an IC card terminal by this approach (** which processes nothing).

[0035] A cryptographic key is changed for every use (whenever an IC card is inserted in an IC card terminal), but with the technique proposed by JP,2-31290,A or JP,2-44389,A, about one use, since it uses the same cryptographic key, a cryptographic key may be decoded, it impersonates after authentication, and it cannot communicate between IC cards while ** is possible for after authentication.

[0036] Since the cryptographic key is changed for every communication link, decode of a cryptographic key becomes difficult, but it will become still more complicated constituting it, if it a configuration not only becomes complicated, but is combined with one of the above-mentioned authentication approaches, since the technique proposed by JP,2-195378,A omits authentication. Moreover, since the configuration and signal processing of an IC card and an IC card terminal are almost the same, although the communication link between IC cards is possible, in order to attest, when it combines with one of the above-mentioned authentication approaches, the communication link between IC cards will be impossible.

[0037] Then, this invention aims at offering the information correspondence procedure and equipment which can also prevent the malfeasance after authentication depended for impersonating, and can perform not only the communication link with an IC card and an IC card terminal but the communication link between IC cards while it prevents decode of a cryptographic key with an easy configuration.

[0038]

[Means for Solving the Problem] In order to attain the purpose mentioned above, in invention of claim 1 In the information correspondence procedure which communicates by repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment In case the 1st information over said 2nd equipment is transmitted from said 1st equipment, while generating the 1st random number with said 1st equipment Compound the 1st generated this random number and this 1st information, and it considers as the 1st synthetic information. this -- said 2nd equipment which enciphered the 1st synthetic information, transmitted to said 2nd equipment as 1st encryption information, and received said 1st encryption information from said 1st equipment It separates into said the 1st information and said 1st random number, after decrypting the 1st this encryption information which received. In case processing to said 1st information is performed and the 2nd information over said 1st equipment is transmitted from said 2nd equipment, while generating the 2nd random number with said 2nd equipment Compound the 2nd generated this random number, this 2nd information, and said 1st separated random number, and it considers as the 2nd synthetic information. this -- said 1st equipment which enciphered the 2nd synthetic information, transmitted to said 1st equipment as 2nd encryption information, and received the 2nd encryption information from said 2nd equipment It separates into said the 2nd information, said 2nd random number, and said 1st random number, after decrypting the 2nd this encryption information which received. When the 1st separated this random number is compared with said 1st generated random number and said 1st separated random number and said 1st generated random number are in agreement with this comparison, attest said 2nd equipment and processing to said 2nd information is performed. In case the 3rd information over said 2nd equipment is transmitted from said 1st equipment, while generating the 3rd random number with said 1st equipment Compound the 3rd generated this random number, this 3rd information, and said 2nd separated random number, and it considers as the 3rd synthetic information. this -- said 2nd equipment which enciphered the 3rd synthetic information, transmitted to said 2nd equipment as 3rd encryption information, and received the 3rd encryption information from said 1st equipment It separates into said the 3rd information, said 3rd random number, and said 2nd random number, after decrypting the 3rd this

encryption information which received. When the 2nd separated this random number is compared with said 2nd generated random number and said 2nd separated random number and said 2nd generated random number are in agreement with this comparison, attest said 1st equipment and processing to said 3rd information is performed. It is characterized by repeating the above-mentioned processing until transmission and reception of the information between said 1st equipment and said 2nd equipment are completed.
[0039] Moreover, in invention of claim 2, it is characterized by being carried out using a cryptographic key with same the encryption and the decryption which said 1st equipment performs, encryption which said 2nd equipment performs, and decryption in invention of claim 1.
[0040] Moreover, in invention of claim 3, in invention of claim 1, said 1st equipment is an IC card and said 2nd equipment is characterized by being said IC card and the IC card terminal which performs an informational communication link.
[0041] Moreover, in invention of claim 4, it is characterized by said the 1st equipment and said 2nd equipment being an IC card in invention of claim 1.
[0042] Moreover, it sets to the information correspondence procedure which communicates in invention of claim 5 by repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment. In case the 1st information over said 2nd equipment is transmitted from said 1st equipment, while generating the 1st random number with said 1st equipment Compound the 1st encryption information and said 1st generated random number, and it transmits to said 2nd equipment as the 1st transmit information. this 1st information -- enciphering -- the 1st encryption information -- carrying out -- this -- Said 2nd equipment which received said 1st transmit information from said 1st equipment After dividing the 1st this transmit information which received into said 1st random number and said 1st encryption information, this, while generating the 2nd random number with said 2nd equipment, in case the 1st encryption information is decrypted to said 1st information, processing to this 1st information is performed and the 2nd information over said 1st equipment is transmitted from said 2nd equipment Compound this 2nd information and said 1st separated random number, and it considers as the 2nd synthetic information. Compound the 2nd encryption information and said 2nd generated random number, and it transmits to said 1st equipment as the 2nd transmit information. this -- the 2nd synthetic information -- enciphering -- the 2nd encryption information -- carrying out -- this -- Said 1st equipment which received the 2nd transmit information from said 2nd equipment After dividing the 2nd this transmit information which received into said 2nd random number and said 2nd encryption information, Decrypt the 2nd encryption information to said 2nd synthetic information, and the 2nd this decrypted synthetic information is divided into said the 1st random number and said 2nd information. this -- When the 1st separated this random number is compared with said 1st generated random number and said 1st separated random number and said 1st generated random number are in agreement with this comparison, attest said 2nd equipment and processing to said 2nd information is performed. In case the 3rd information over said 2nd equipment is transmitted from said 1st equipment, while generating the 3rd random number with said 1st equipment Compound this 3rd information and said 2nd separated random number, and it considers as the 3rd synthetic information. Compound the 3rd encryption information and said 3rd generated random number, and it transmits to said 2nd equipment as the 3rd transmit information. this -- the 3rd synthetic information -- enciphering -- the 3rd encryption information -- carrying out -- this -- Said 2nd equipment which received the 3rd transmit information from said 1st equipment After dividing the 3rd this transmit information which received into said 3rd random number and said 3rd encryption information, Decrypt the 3rd encryption information to said 3rd synthetic information, and the 3rd this decrypted synthetic information is divided into said the 2nd random number and said 3rd information. this -- When the 2nd separated this random number is compared with said 2nd generated random number and said 2nd separated random number and said 2nd generated random number are in agreement with this comparison, attest said 1st equipment and processing to said 3rd information is performed. It is characterized by repeating the above-mentioned processing until transmission and reception of the information between said 1st equipment and said 2nd equipment are completed.
[0043] Moreover, in invention of claim 6, it is characterized by being carried out using a cryptographic key with same the encryption and the decryption which said 1st equipment performs, encryption which said 2nd equipment performs, and decryption in invention of claim 5.

[0044] Moreover, in invention of claim 7, in invention of claim 5, said 1st equipment is an IC card and said 2nd equipment is characterized by being said IC card and the IC card terminal which performs an informational communication link.

[0045] Moreover, in invention of claim 8, it is characterized by said the 1st equipment and said 2nd equipment being an IC card in invention of claim 5.

[0046] In the information communication device which communicates in invention of claim 9 by repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment moreover, said 1st equipment The 1st information processing means, the 1st random-number-generation means, the 1st synthetic means, the 1st encryption means, the 1st decryption means, the 1st separation means, and the 1st comparison means are provided. Said 2nd equipment The 2nd information processing means, the 2nd random-number-generation means, the 2nd synthetic means, the 2nd encryption means, the 2nd decryption means, the 2nd separation means, and the 2nd comparison means are provided. When said 1st equipment transmits information to said 2nd equipment While outputting the information which said 1st information processing means transmits, said 1st random-number-generation means generates a random number. The random number which said 2nd equipment contained in information just before said 1st separation means received from said 2nd equipment generated is separated and acquired. After compounding the information which said 1st information processing means outputted, the random number which said 1st random-number-generation means generated, and the random number which said 1st separation means acquired with said 1st synthetic means, When it enciphers with said 1st encryption means, it transmits as encryption information and said 2nd equipment transmits information to said 1st equipment While outputting the information which said 2nd information processing means transmits, said 2nd random-number-generation means generates a random number. The random number which said 1st equipment contained in information just before said 2nd separation means received from said 1st equipment generated is separated and acquired. After compounding the information which said 2nd information processing means outputted, the random number which said 2nd random-number-generation means generated, and the random number which said 2nd separation means acquired with said 2nd synthetic means, When it enciphers with said 2nd encryption means, it transmits as encryption information and said 1st equipment receives the encryption information from said 2nd equipment It separates into the information which said 2nd information processing means outputted with said 1st separation means, the random number which said 2nd random-number-generation means generated, and the random number which said 2nd separation means acquired, after decrypting the received this encryption information with said 1st decryption means. Said 1st comparison means compares the acquired this random number and the random number which said 1st random-number-generation means generated. The information which said 2nd information processing means separated with said 1st separation means when this comparison result was coincidence outputted is processed with said 1st information processing means. When said 2nd equipment receives the encryption information from said 1st equipment It separates into the information which said 1st information processing means outputted with said 2nd separation means, the random number which said 1st random-number-generation means generated, and the random number which said 1st separation means acquired, after decrypting the received this encryption information with said 2nd decryption means. It is characterized by processing the information which said 1st information processing means which compared the acquired this random number with the random number which said 2nd random-number-generation means generated with said 2nd comparison means, and was separated with said 2nd separation means when this comparison result was coincidence outputted with said 2nd information processing means.

[0047] moreover, in transmitting information to said 2nd equipment in invention of claim 9 in invention of claim 10 before said 1st equipment receives information from said 2nd equipment Said 1st synthetic means compounds only the information which said 1st information processing means outputted, and the random number which said 1st random-number-generation means generated. In transmitting information to said 1st equipment before said 2nd equipment receives information from said 1st equipment Said 2nd synthetic means compounds only the information which said 2nd information processing means outputted, and the random number which said 2nd random-number-generation means generated. When information is received from said 2nd equipment before said 1st equipment transmitted information to said 2nd equipment The information which said 2nd information processing means separated with said

1st separation means, without said 1st comparison means comparing a random number outputted is processed with said 1st information processing means. When information is received from said 1st equipment before said 2nd equipment transmitted information to said 1st equipment It is characterized by processing the information which said 1st information processing means separated with said 2nd separation means, without said 2nd comparison means comparing a random number outputted with said 2nd information processing means.

[0048] Moreover, in invention of claim 11, it is characterized by using a cryptographic key with same said 1st encryption means, said 2nd encryption means, said 1st decryption means, and said 2nd decryption means in invention of claims 9 or 10.

[0049] Moreover, in invention of claim 12, in invention of claims 9 or 10, said 1st equipment is an IC card and said 2nd equipment is characterized by being said IC card and the IC card terminal which performs an informational communication link.

[0050] Moreover, in invention of claim 13, it is characterized by said the 1st equipment and said 2nd equipment being an IC card in invention of claims 9 or 10.

[0051] In the information communication device which communicates in invention of claim 14 by repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment moreover, said 1st equipment The 1st information processing means, the 1st random-number-generation means, the 1st upper composition means, the 1st lower layer composition means, the 1st encryption means, the 1st decryption means, the 1st upper separation means, the 1st lower layer separation means, and the 1st comparison means are provided. Said 2nd equipment possesses the 2nd information processing means, the 2nd random-number-generation means, the 2nd upper composition means, the 2nd lower layer composition means, the 2nd encryption means, the 2nd decryption means, the 2nd upper separation means, the 2nd lower layer separation means, and the 2nd comparison means. When said 1st equipment transmits information to said 2nd equipment While outputting the information which said 1st information processing means transmits, said 1st random-number-generation means generates a random number. The random number which said 2nd equipment contained in information just before said 1st separation means received from said 2nd equipment generated is separated and acquired. After compounding the information which said 1st information processing means outputted, and the random number which said 1st separation means acquired with said 1st lower layer composition means, Encipher with said 1st encryption means, consider as encryption information, and it transmits as synthetic information which compounded this encryption information and the random number which said 1st random-number-generation means generated with said 1st upper composition means. When said 2nd equipment transmits information to said 1st equipment While outputting the information which said 2nd information processing means transmits, said 2nd random-number-generation means generates a random number. The random number which said 1st equipment contained in information just before said 2nd separation means received from said 1st equipment generated is separated and acquired. After compounding the information which said 2nd information processing means outputted, and the random number which said 2nd separation means acquired with said 2nd lower layer composition means, Encipher with said 2nd encryption means, consider as encryption information, and it transmits as synthetic information which compounded this encryption information and the random number which said 2nd random-number-generation means generated with said 2nd upper composition means. When said 1st equipment receives the synthetic information from said 2nd equipment After said 1st upper separation means separates the random number which said 2nd random-number-generation means generated from the received this synthetic information, It separates into the information which decrypted with said 1st decryption means and said 2nd information processing means outputted with said 1st separation means further, and the random number which said 2nd separation means acquired. Said 1st comparison means compares the acquired this random number and the random number which said 1st random-number-generation means generated. The information which said 2nd information processing means separated with said 1st separation means when this comparison result was coincidence outputted is processed with said 1st information processing means. When said 2nd equipment receives the synthetic information from said 1st equipment After said 2nd upper separation means separates the random number which said 1st random-number-generation means generated from the received this synthetic information, It separates into the information which decrypted with said 2nd decryption means and said 1st information processing

means outputted with said 2nd separation means further, and the random number which said 1st separation means acquired. It is characterized by processing the information which said 1st information processing means which compared the acquired this random number with the random number which said 2nd random-number-generation means generated with said 2nd comparison means, and was separated with said 2nd separation means when this comparison result was coincidence outputted with said 2nd information processing means.
[0052] moreover, in transmitting information to said 2nd equipment in invention of claim 14 in invention of claim 15 before said 1st equipment receives information from said 2nd equipment Said 1st encryption means enciphers only the information which said 1st information processing means outputted. In transmitting information to said 1st equipment before said 2nd equipment receives information from said 1st equipment Said 2nd encryption means enciphers only the information which said 2nd information processing means outputted. When information is received from said 2nd equipment before said 1st equipment transmitted information to said 2nd equipment The information which said 2nd information processing means separated with said 1st separation means, without said 1st comparison means comparing a random number outputted is processed with said 1st information processing means. When information is received from said 1st equipment before said 2nd equipment transmitted information to said 1st equipment It is characterized by processing the information which said 1st information processing means separated with said 2nd separation means, without said 2nd comparison means comparing a random number outputted with said 2nd information processing means.
[0053] Moreover, in invention of claim 16, it is characterized by using a cryptographic key with same said 1st encryption means, said 2nd encryption means, said 1st decryption means, and said 2nd decryption means in invention of claims 14 or 15.
[0054] Moreover, in invention of claim 17, in invention of claims 14 or 15, said 1st equipment is an IC card and said 2nd equipment is characterized by being said IC card and the IC card terminal which performs an informational communication link.
[0055] Moreover, in invention of claim 18, it is characterized by said the 1st equipment and said 2nd equipment being an IC card in invention of claims 14 or 15.
[0056]
[Embodiment of the Invention] Hereafter, the information correspondence procedure concerning this invention and one example of equipment are explained to a detail with reference to an accompanying drawing.
[0057] Drawing 1 is the block diagram showing the IC card structure of a system. In drawing 1 , the IC card terminal 1 possesses the random-number-generation means 11, a random number and a merge means 12, the encryption means 13, the comparison means 14, the data-processing means 15, the cryptographic key storing means 16, a random number and a data separation means 17, and the decryption means 18, and is constituted. IC card 2 possesses the random-number-generation means 21, a random number and a merge means 22, the encryption means 23, the comparison means 24, the data-processing means 25, the cryptographic key storing means 26, a random number and a data separation means 27, and the decryption means 28, and is constituted.
[0058] In the IC card terminal 1, the data-processing means 15 processes generating processing of the data which deliver and receive between IC cards 2, and ********** to IC card 2 etc., the random-number-generation means 11 generates the random number of arbitration, and a random number and the merge means 12 compound the random number which the random-number-generation means 11 generates, the data which the data-processing means 15 outputs. This composition may be compounded based on a predetermined regulation so that it may serve as encryption, but since encryption is performed in the latter part, the composition which is only connected extent is enough as it. The encryption means 13 performs encryption processing using the random number compounded with the random number and the merge means 12, and the cryptographic key in which data etc. are stored by the cryptographic key storing means 16. The decryption means 18 carries out decryption processing using the cryptographic key in which the cipher transmitted from IC card 2 is stored by the cryptographic key storing means 16, and a random number and the data separation means 17 divide into a random number and data the information decrypted with the decryption means 18. The comparison means 14 compares the random number which the random-number-generation means 11 generated with the random number which performed predetermined processing later mentioned by these random numbers, and when the

same (it will become the same if the predetermined processing mentioned later is made justly), it operates so that IC card 2 may be attested and data processing may be permitted to the data-processing means 15.
[0059] In IC card 2, similarly, the data-processing means 25 processes generating processing of the data which deliver and receive between the IC card terminals 1, and ********** to the IC card terminal 1, etc., the random-number-generation means 21 generates the random number of arbitration, and a random number and the merge means 22 compound the random number which the random-number-generation means 21 generates, the data which the data-processing means 25 outputs. The encryption means 23 performs encryption processing using the random number compounded with the random number and the merge means 22, and the cryptographic key in which data etc. are stored by the cryptographic key storing means 26. The cryptographic key stored in the cryptographic key storing means 26 is the same as that of the cryptographic key which the cryptographic key storing means 16 of the IC card terminal 1 stores. The decryption means 28 carries out decryption processing using the cryptographic key in which the cipher transmitted from the IC card terminal 1 is stored by the cryptographic key storing means 26, and a random number and the data separation means 27 divide into a random number and data the information decrypted with the decryption means 28. The comparison means 24 compares the random number which the random-number-generation means 21 generated with the random number which performed predetermined processing later mentioned by these random numbers, and when the same, it operates so that the IC card terminal 1 may be attested and data processing may be permitted to the data-processing means 25.
[0060] Drawing 2 is drawing having shown actuation of IC card system shown in drawing 1 , and the flow of a signal.
[0061] First, if a user inserts IC card 2 in the IC card terminal 1 and both are connected electrically, the IC card terminal 1 will generate a random number R1 with the random-number-generation means 11, and will encipher a random number R1 with the encryption means 13 (step 51). At this time, after a random number R1 is compounded with the random-number demand which is a random-number-generation demand which receives to IC card 2 which the data-processing means 15 outputted with the random number and the merge means 12, it is enciphered using the cryptographic key stored in the cryptographic key storing means 16 with the encryption means 13.
[0062] The random number R1 and the random-number demand K (the random-number demand, R1) which were enciphered are sent out to IC card 2 (step 52), in IC card 2, are decrypted using the cryptographic key in which this is stored by the cryptographic key storing means 26 with the decryption means 28, and process received data with the data-processing means 25 through a random number and the data separation means 27 (step 53).
[0063] Next, based on the processing result of received data (based on a demand of the IC card terminal 1), the random-number-generation means 21 generates a random number R2 with the data-processing means 25. K (a response, R1R2) which compounded the reply signal over this, a random number R1, and a random-number demand with the random number and the merge means 22, and enciphered this using the cryptographic key storing means 16 with the encryption means 23 is sent out to (step 53) and the IC card terminal 1 (step 54).
[0064] The IC card terminal 1 which received K (a response, R1R2) decrypts this using the cryptographic key stored in the cryptographic key storing means 16 with the decryption means 18, separates a random number R1 with a random number and the data separation means 17, and passes delivery, and a reply signal and a random number R2 to the comparison means 14 to the data-processing means 15. With the comparison means 14, if the random number R1 separated with the random number and the data separation means 17 is compared with the random number R1 which the random-number-generation means 11 generated at step 51 and both are in agreement, IC card 2 will be attested and processing of data etc. will be permitted to the data-processing means 15. However, the authorization given to the data-processing means 15 here is only processing to the reply signal received with the random number R1 separated with the random number and the data separation means 17.
[0065] Attesting IC card 2, when the random-number-generation means 11 is in agreement at the random number R1 and step 51 which were separated with the random number and the data separation means 17 compared with the comparison means 14 That the demand and response to the IC card terminal 1 are transmitted with a random number R1 It is a reason for being impossible in addition to the

partner who has the cryptographic key stored in the cryptographic key storing means 16. IC card terminal 1 self transmits the demand and response which are sent to coincidence even if it has answered a letter as it is in the random number R1 which the IC card terminal 1 enciphered and the inaccurate partner who does not have a cryptographic key temporarily transmitted, and an unjust demand is because it does not enter.

[0066] Next, a data-processing means 15 by which data processing was permitted Generate the access request to IC card 2, and this and the received random number R2 to a random number and the merge means 12 Delivery, A random number and the merge means 12 compound the random number R3 which this and the random-number-generation means 11 generated. To the encryption means 13 Delivery, It enciphers using the cryptographic key in which this is stored by the cryptographic key storing means 16, and the encryption means 13 is sent out to (step 55) and IC card 2 as K (an access request, R2R3) (step 56).

[0067] IC card 2 which received K (an access request, R2R3) decrypts this using the cryptographic key stored in the cryptographic key storing means 26 with the decryption means 28, separates a random number R2 with a random number and the data separation means 27, and passes delivery, and a reply signal and a random number R3 to the comparison means 24 to the data-processing means 25. With the comparison means 24, if the random number R2 separated with the random number and the data separation means 27 is compared with the random number R2 which the random-number-generation means 21 generated at step 53 and both are in agreement, the IC card terminal 1 will be attested and processing of data etc. will be permitted to the data-processing means 25. The above-mentioned IC card terminal 1 of the reason for attesting the IC card terminal 1 by comparison with the comparison means 24 is the same as that of the reason for having attested IC card 2.

[0068] The data-processing means 25 will generate the access result to the IC card terminal 1, if data processing is permitted. The random number R4 with which, as for delivery, the random number, and the merge means 22, this and the random-number-generation means 21 generated this and the received random number R3 to the random number and the merge means 22 is compounded. To the encryption means 23 Delivery, It enciphers using the cryptographic key in which this is stored by the cryptographic key storing means 26, and the encryption means 23 is sent out to (step 57) and the IC card terminal 1 as K (an access result, R3R4) (step 58).

[0069] The IC card terminal 1 which received K (an access result, R3R4) decrypts this using the cryptographic key stored in the cryptographic key storing means 16 with the decryption means 18, separates a random number R3 with a random number and the data separation means 17, and passes delivery, and a reply signal and a random number R4 to the comparison means 14 to the data-processing means 15. With the comparison means 14, if the random number R3 separated with the random number and the data separation means 17 is compared with the random number R3 which the random-number-generation means 11 generated at step 55 and both are in agreement, IC card 2 will be attested and processing of data etc. will be permitted to the data-processing means 15. The data-processing means 15 will generate the directions or data M4 to IC card 2, if IC card 2 is attested by the comparison means 14. The random number R5 with which, as for delivery, the random number, and the merge means 12, this and the random-number-generation means 11 generated this and the received random number R4 to the random number and the merge means 12 is compounded. To the encryption means 13 Delivery, It enciphers using the cryptographic key in which this is stored by the cryptographic key storing means 16, and the encryption means 13 is sent out to (step 59) and IC card 2 as K (M4, R4R5) (step 60).

[0070] IC card 2 which received K (M4, R4R5) decrypts this using the cryptographic key stored in the cryptographic key storing means 26 with the decryption means 28, separates a random number R4 with a random number and the data separation means 27, and passes delivery, and a reply signal and a random number R5 to the comparison means 24 to the data-processing means 25. With the comparison means 24, if the random number R4 separated with the random number and the data separation means 27 is compared with the random number R4 which the random-number-generation means 21 generated at step 57 and both are in agreement, the IC card terminal 1 will be attested and processing of data etc. will be permitted to the data-processing means 25. The data-processing means 25 will generate the command or data M5 to the IC card terminal 1, if the IC card terminal 1 is attested by the comparison means 24. The random number R6 with which, as for delivery, the random number, and the merge means

22, this and the random-number-generation means 21 generated this and the received random number R5 to the random number and the merge means 22 is compounded. To the encryption means 23 Delivery, It enciphers using the cryptographic key in which this is stored by the cryptographic key storing means 26, and the encryption means 23 is sent out to (step 61) and the IC card terminal 1 as K (M5, R5R6) (step 62).

[0071] Like the following, the IC card terminal 1 processes, after attesting IC card 2 by the comparison of a random number R5 (step 63). Transmit K (M6, R6R7) to IC card 2 (step 64), and IC card 2 processes, after attesting the IC card terminal 1 by the comparison of a random number R6 (step 65). K (M7, R7R8) is transmitted to the IC card terminal 1 (step 66), and it repeats until a communication link ends this.

[0072] thus, the thing which the IC card terminal 1 and IC card 2 attest mutually for every communication link -- impersonating -- etc. -- injustice is prevented. Moreover, since the ciphers which have changed the cryptographic key as a result each time, that is, encipher the same plaintext (information which should communicate essentially) and are acquired since it is enciphering by compounding a random number to the information (a random-number demand, a response, an access request, an access result, M1, M2 grade) which should communicate essentially differ each time for the compounded random number, it becomes difficult [decode of a cipher, or unjust acquisition of a cryptographic key] very much [them].

[0073] In addition, the same effectiveness can be acquired, even if it constitutes so that the random number transmitted first may be compounded with (R4 grade of 52 stepR1, 54 stepR2, 56 stepR3, and step 58), and other information enciphered without enciphering, for example, it may carry out like K (access request, R2)R3 at step 56 and it may transmit after being generated.

[0074] Next, the information correspondence procedure of IC card system concerning this invention and the 2nd example of equipment are explained.

[0075] Drawing 3 is the block diagram showing the IC card structure of a system in the case of performing the information communication link between IC cards. In drawing 3 IC card A2-1 the random-number-generation means 21-1, a random number and a merge means 22-1, the encryption means 23-1, the comparison means 24-1, the data-processing means 25-1, the cryptographic key storing means 26-1, a random number and a data separation means 27-1, and the decryption means 28-1 IC card B-2 -2 possesses the random-number-generation means 21-2, a random number and a merge means 22-2, the encryption means 23-2, the comparison means 24-2, the data-processing means 25-2, the cryptographic key storing means 26-2, a random number and a data separation means 27-2, and the decryption means 28-2, and is constituted. It connects through the IC card terminal 3.

[0076] In case data are communicated between this IC card A2-1 and IC card B-2 -2, since authentication and data communication are performed, explanation is omitted like the case where the communication link between the IC card terminal 1 explained in the 1st above-mentioned example and IC card 2 is performed.

[0077] Moreover, although IC card A2-1 and IC card B-2 -2 are connected through the IC card terminal 3, the IC card terminal 3 performs only actuation which passes the other party data, without processing the data which IC card A2-1 and IC card B-2 -2 sent out.

[0078] This IC card A2-1 and IC card B-2 -2 are the same configuration as IC card 2 explained in the above-mentioned example, and not only the data communication between IC cards but data communication with the IC card terminal 1 shown in drawing 1 is possible for them.

[0079]

[Effect of the Invention] As explained above, according to this invention, an IC card terminal and an IC card perform encryption processing, and communicate information. An IC card terminal The random number currently compounded by the information received from the IC card processes information which attested the IC card and was received only when equal to the random number compounded to the information previously transmitted to the IC card from the IC card terminal. since it constituted so that information received after the IC card attested the IC card terminal similarly might be processed, while being able to prevent leakage of the cryptographic key by tapping etc. -- "-- it can impersonate and malfeasances, such as" action, can also be prevented.

[0080] Moreover, since the IC card terminal and the IC card were provided and the same means was constituted, data communication between IC cards can also be performed through the IC card terminal

which does not have a data-processing device.

[Translation done.]

TECHNICAL FIELD

[Field of the Invention] About an information correspondence procedure and equipment, especially this invention relates to the information correspondence procedure and equipment which can communicate between an IC card and an IC card terminal and between IC cards while preventing leakage of a cryptographic key.

[Translation done.]

PRIOR ART

[Description of the Prior Art] As compared with a magnetic card, the informational storage capacity of the IC card which carried IC (integrated circuit: integrated circuit) is large, and since it is possible to also make an operation etc. process inside an IC card, the application is various.
[0003] In the case where money information and extra sensitive information are treated depending on this application, for example, the adoption of an information correspondence procedure with high safeties, such as authentication and informational encryption, or equipment including an IC card and its peripheral device serves as important requirements.
[0004] Here, the conventional information correspondence procedure in an IC card and its peripheral device and an example of equipment are explained.
[0005] Drawing 4 is drawing having shown the flow of the block diagram having shown an example of the conventional IC card system, and a signal. As for the IC card terminal 101, the conventional IC card system possesses the confidential information storing means (KEY2) 119, the processing means 115, the encryption means (EK2) 113, and a decryption means (DK1), as shown in drawing 4 (a), and IC card 102 possesses the confidential information storing means (KEY1) 129, the comparison means 124, the processing means 125, the encryption means (EK1) 123, and the decryption means (DK2) 128, and is constituted.
[0006] Actuation in case the IC card terminal 101 performs the writing and read-out of information to IC card 102 here is explained.
[0007] If IC card 102 is inserted in the IC card terminal 101, the confidential information (KEY2) by which the IC card terminal 101 is stored in the confidential information storing means (KEY2) 119 will be transmitted to IC card 102 (step 151). IC card 102 will perform comparison collating for the confidential information (KEY1) stored in this and the confidential information storing means (KEY1) 129 with the comparison means 124, if confidential information (KEY2) is received. If confidential information (KEY2) is in agreement with confidential information (KEY1), IC card 102 will attest the IC card terminal 101 with it being a just IC card terminal, and will permit processing actuation to the processing means 125. Although the processing means 125 will start the communication link of the processing means 115 and data of the IC card terminal 101, an instruction, etc. if actuation is permitted In case it communicates, the data transmitted from the processing means 125 (M1, M3) It is enciphered and transmitted with the encryption means (EK1) 123 (steps 152 and 154), and the IC card terminal 101 decrypts this with the decryption means (DK1) 118, and the processing means 115 processes. Moreover, it is enciphered with the encryption means (EK2) 113 (M2, M4), and the data transmitted from the processing means 115 are transmitted (steps 153 and 155), IC card 102 decrypts this with the decryption means (DK2) 128, and the processing means 125 processes.
[0008] Although the cryptographic key which the encryption means (EK1) 123 and the decryption means (DK1) 118 use needs to be the same and the cryptographic key which the encryption means (EK2) 113 and the decryption means (DK2) 128 use needs to be the same in order to perform such processing, four persons' cryptographic key may be the same. Moreover, the confidential information storing means (KEY2) 119 is constituted from input means, such as a personal identification number, and you may make it IC card 102 attest the user who operates the IC card terminal 101.
[0009] However, in the configuration shown in drawing 4 , it is monitoring the communication link between the IC card terminal 101 and IC card 102, and the problem of becoming it being possible to

carry out the unjust acquisition of the confidential information comparatively easily, and possible to use rewriting and the forged IC card of the information on IC card 102 if confidential information is acquired arises.

[0010] Moreover, since the enciphered information is also always communicating using the same cryptographic key, possibility of decoding is high.

[0011] In order to cope with such a problem, while attesting without communicating confidential information between an IC card terminal and an IC card, the technique of preventing from decoding the enciphered information easily is proposed by JP,2-31289,A, JP,2-31290,A, JP,2-44389,A, JP,2-195378,A, etc.

[0012] The technique proposed by JP,2-31289,A The IC card terminal 201 which possesses the processing means 215, the encryption means (EK2) 213-1, the encryption means (EK4) 213-2, the decryption means (DK1) 218-1, and the decryption means (DK3) 218-2 as shown in drawing 5 (a), It consists of IC cards 202 possessing the processing means 225, the random-number-generation means (R) 221, the comparison means 224, the encryption means (EK1) 223-1, the encryption means (EK3) 223-2, the decryption means (DK2) 228-1, and the decryption means (DK4) 228-2.

[0013] This IC card system delivers and receives a signal by flow as shown in drawing 5 (b). First, in order that IC card 202 may attest the IC card terminal 201 Generate a random number (R) with the random-number-generation means (R) 221, encipher this with the encryption means (EK1) 223-1, and it transmits to the IC card terminal 201 (step 251). The IC card terminal 201 decrypts this with the decryption means (DK1) 218-1, enciphers the decrypted random number (R) with the encryption means (EK2) 213-1, and transmits it to IC card 202 (step 252).

[0014] an IC card -- 202 -- having received -- coding information -- a decryption -- a means (DK2) -- 228 - one -- decrypting -- this -- a decryption -- having obtained -- a random number -- (-- R --) -- random number generation -- a means -- (-- R --) -- 221 -- having generated -- a random number -- (-- R --) -- a comparison -- a means -- 224 -- comparing -- both -- being in agreement -- if -- the IC card terminal 201 -- attesting -- the processing means 225 -- authorization of operation -- giving .

[0015] This attests the IC card terminal 201 by the random number which IC card 202 generated and was transmitted having been answered by being carried out in just processing, and when the encryption means (EK1) 223-1 and the decryption means (DK1) 218-1 use the same cryptographic key and the encryption means (EK2) 213-1 and the decryption means (DK2) 228-1 are using the same cryptographic key, it is materialized. However, the cryptographic key which the encryption means (EK1) 223-1 and the encryption means (EK2) 213-1 use in this case must not be the same.

[0016] Although the processing means 225 will start the communication link of the processing means 215 and data of the IC card terminal 201, an instruction, etc. if IC card 202 attests the IC card terminal 201 and permits actuation of the processing means 225 In case it communicates, the data transmitted from the processing means 225 (M1, M3) It is enciphered and transmitted with the encryption means (EK3) 223-2 (steps 253 and 255), and the IC card terminal 201 decrypts this with the decryption means (DK3) 218-2, and the processing means 215 processes. Moreover, it is enciphered with the encryption means (EK4) 213-2 (M2, M4), and the data transmitted from the processing means 215 are transmitted (steps 254 and 256), IC card 202 decrypts this with the decryption means (DK4) 228-2, and the processing means 225 processes.

[0017] In this case, without transmitting confidential information directly unlike the system explained by drawing 4 , it is enciphering the random number used at the time of authentication by the cryptographic key, and the information acquired by wire tapping is changed each time, and it is going to make decode of a code difficult.

[0018] The technique proposed by JP,2-31290,A The IC card terminal 301 which possesses the processing means 315, the encryption means (EK2) 313-1, encryption means (ER)313-2, the decryption means (DK1) 318-1, and decryption means (DR)318-2 as shown in drawing 6 (a), It consists of the processing means 325, the random-number-generation means (R) 321, the comparison means 324, the encryption means (EK1) 323-1, encryption means (ER)323-2, a decryption means (DK2) 328-1, and IC card 302 possessing decryption means (DR)328-2.

[0019] Although this IC card system delivers and receives a signal by flow as shown in drawing 6 (b), since the approach IC card 302 attests the IC card terminal 301 with the signal delivered and received at steps 351 and 352 is the same as that of the case where it is shown in drawing 5 , explanation is

omitted.

[0020] Now, although the processing means 325 will start the communication link of the processing means 315 and data of the IC card terminal 301, an instruction, etc. if IC card 302 attests the IC card terminal 301 and actuation of the processing means 325 is permitted In case it communicates, the data transmitted from the processing means 325 (M1, M3) Encryption means (ER) By 323-2, at the time of authentication, the random number which the random-number-generation means (R) 321 generated is enciphered as a cryptographic key, and it is transmitted (steps 353 and 355), and the IC card terminal 301 decrypts this by decryption means (DR)318-2, and the processing means 315 processes. Moreover, the random number (it memorizes at the time of authentication) which the random-number-generation means (R) 321 generated in encryption means (ER)313-2 similarly at the time of authentication (M2, M4) is enciphered as a cryptographic key, the data transmitted from the processing means 315 are transmitted (steps 354 and 356), IC card 302 decrypts this by decryption means (DR)328-2, and the processing means 325 processes.

[0021] In this case, by using the random number which generated the encryption at the time of communicating data etc. at the time of authentication as a cryptographic key in addition to the system explained by drawing 5 , a cryptographic key is changed each time and it is going to make decode difficult.

[0022] Moreover, the technique proposed by JP,2-44389,A Drawing 7 As shown in (a), the processing means 415, a random-number-generation means (R2) 411, the comparison means 414, the synthetic means 412, the encryption means (EK2) 413-1, the encryption means (ER one R2) 413-2, the decryption means (DK1) 418-1, the decryption means (DK2) 418-2, and the decryption means (DR one R2) 418-3 The IC card terminal 401 to provide, The processing means 425, a random-number-generation means (R1) 421, the comparison means 424, the separation means 427, the encryption means (EK1) 423-1, the encryption means (EK3) 423-2, the encryption means (ER one R2) 423-3, the decryption means (DK2) 428-1, and the decryption means (DR one R2) 428-2 It consists of IC cards 402 to provide.

[0023] This IC card system delivers and receives a signal by flow as shown in drawing 7 (b). First, in order to attest the IC card terminal 401, IC card 402 generates a random number (R1) with the random-number-generation means (R1) 421, enciphers this with the encryption means (EK1) 423-1, and transmits it to the IC card terminal 401 (step 451). While decrypting the received encryption information with the decryption means (DK1) 418-1, in order to attest IC card 402, the IC card terminal 401 generates a random number (R2) with the random-number-generation means (R2) 411, compounds this random number (R2) and the decrypted random number (R1) with the synthetic means 412, enciphers this with the encryption means (EK2) 413-1, and transmits it to IC card 402 (step 452).

[0024] IC card 402 decrypts the coding information which received with the decryption means (DK2) 428-1, and divides it into a random number (R1) and a random number (R2) with the separation means 427 further. If it is compared by the random number (R1) and the comparison means 424 which the random-number-generation means (R1) 421 generated and both are in agreement, the separated random number (R1) will attest the IC card terminal 401, and will give authorization of operation to the processing means 425.

[0025] On the other hand, the random number (R2) separated with the separation means 427 It is enciphered with the encryption means (EK3) 423-2, and is transmitted to the IC card terminal 401. The IC card terminal 401 The comparison means 414 compares the random number (R2) which decrypted the coding information which received with the decryption means (DK3) 418-2, and was obtained by the decryption, and the random number (R2) which the random-number-generation means (R2) 411 generated. If both are in agreement, IC card 402 will be attested and authorization of operation will be given to the processing means 415.

[0026] Although the processing means 415 and the processing means 425 will start the communication link of data, an instruction, etc. mutually if IC card 402 attests the IC card terminal 401, actuation of the processing means 425 is permitted, the IC card terminal 401 attests IC card 402 and actuation of the processing means 415 is permitted In case it communicates, the data which the processing means 425 transmits (M1, M3) With the encryption means (ER one R2) 423-3, at the time of authentication, encipher the random number (R1) which the random-number-generation means (R1) 421 generated, and the random number (R2) which the random-number-generation means (R2) 411 generated as a cryptographic key, and it is transmitted (steps 454 and 456). The IC card terminal 401 decrypts this with the

decryption means (DR one R2) 418-3, and the processing means 415 processes. Moreover, the data transmitted from the processing means 415 (M2, M4) Similarly, with the encryption means (ER one R2) 413-2, at the time of authentication, encipher the random number (R1) which the random-number-generation means (R1) 421 generated, and the random number (R2) which the random-number-generation means (R2) 411 generated as a cryptographic key, and it is transmitted (steps 455 and 457). IC card 402 decrypts this with the decryption means (DR one R2) 428-2, and the processing means 425 processes.

[0027] As compared with the system which explained this system by drawing 6 , it differs in an IC card not only attests an IC card terminal, but that the IC card terminal has attested the IC card.

[0028] The technique proposed by JP,2-195378,A Drawing 8 As shown in (a), the processing means 515, a random-number-generation means (R2) 511, the encryption means (EK2) 513-1, the encryption means (ER2) 513-2, the decryption means (DK1) 518-1, the decryption means (DR2) 518-2, a register 531-1,531-2, and the EXCLUSIVE-OR-operation means 532-1,532-2 The IC card terminal 501 to provide, The processing means 525, a random-number-generation means (R1) 521, the encryption means (EK1) 523-1, the encryption means (ER2) 523-2, the decryption means (DK2) 528-1, the decryption means (DR2) 528-2, a register 541-1,541-2, and the EXCLUSIVE-OR-operation means 542-1,542-2 It consists of IC cards 502 to provide.

[0029] Especially authentication is not performed although this IC card system delivers and receives a signal by flow as shown in drawing 8 (b).

[0030] First, in advance of the communication link of data etc., IC card 502 generates a random number (R1) with the random-number-generation means (R1) 521. While storing this in a register 541-1,541-2, encipher with the encryption means (EK1) 523-1, and it transmits to the IC card terminal 501 (step 551). The IC card terminal 501 stores in a register 531-1,531-2 the random number (R1) which decrypted and obtained this with the decryption means (DK1) 518-1. Moreover, the IC card terminal 501 generates a random number (R2) with the random-number-generation means (R2) 511, this is enciphered with the encryption means (EK2) 513-1, and it transmits to IC card 502 (step 552), and IC card 502 decrypts this with a decryption means (DK2), and obtains a random number (R2).

[0031] Thus, although the IC card terminal 501 and IC card 502 will start the communication link of data, an instruction, etc. using a random number (R1) and a random number (R2) if a random number (R1) and a random number (R2) are notified mutually In case it communicates, the data transmitted from the processing means 525 (M1, M3, M5) A random number (R2) is enciphered as a cryptographic key with the encryption means (ER2) 523-2, an exclusive OR with the random number (R1) which is the contents further stored in the register 541-1 with the EXCLUSIVE-OR-operation means 542-1 calculates, and this result of an operation is transmitted (step 553). The IC card terminal 501 performs the reverse operation of the operation in the EXCLUSIVE-OR-operation means 542-1 using the random number (R1) which is the contents in which the coding information which received is stored by the register 531-1 with the EXCLUSIVE-OR-operation means 532-1, a random number (R2) is decrypted as a cryptographic key with the decryption means (DR2) 518-2, and the processing means 515 processes this. Moreover, the contents stored in a register 531-1,541-1 are changed into the data (M1) which were the contents of a communication link after a communication link, and an exclusive OR with data (M1) calculates them by the next communication link (step 555).

[0032] Similarly, the data transmitted from the processing means 515 use a random number (R2) for a cryptographic key (M2, M4, M6), and an exclusive OR with the contents of storing of a register 531-1 calculates, and is transmitted.

[0033] Since this system serves as that the cryptographic key is changed for every communication link by the operation of an exclusive OR, and consent, decode of encryption information is difficult.

[Translation done.]

EFFECT OF THE INVENTION

[Effect of the Invention] As explained above, according to this invention, an IC card terminal and an IC card perform encryption processing, and communicate information. An IC card terminal The random number currently compounded by the information received from the IC card processes information which attested the IC card and was received only when equal to the random number compounded to the information previously transmitted to the IC card from the IC card terminal. since it constituted so that information received after the IC card attested the IC card terminal similarly might be processed, while being able to prevent leakage of the cryptographic key by tapping etc. -- "-- it can impersonate and malfeasances, such as" action, can also be prevented.
[0080] Moreover, since the IC card terminal and the IC card were provided and the same means was constituted, data communication between IC cards can also be performed through the IC card terminal which does not have a data-processing device.

[Translation done.]

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] However, with the technique proposed by JP,2-31289,A, since it is always communicating using the same cryptographic key after attesting, the same cipher may communicate and decode of a cryptographic key may be performed. For example, if the same cryptographic key is used to the plaintext which communicates each time [, such as an access request and an access permission,], the always same cipher will communicate. If the cryptographic key after authentication is decoded, after an IC card attests an IC card terminal, it intervenes in a communication link, and a just IC card terminal will be impersonated and unjust access to an IC card will be attained. Moreover, since the configuration or signal processing of an IC card and an IC card terminal are not the same, it cannot communicate between IC cards, without minding an IC card terminal by this approach (** which processes nothing).
[0035] A cryptographic key is changed for every use (whenever an IC card is inserted in an IC card terminal), but with the technique proposed by JP,2-31290,A or JP,2-44389,A, about one use, since it uses the same cryptographic key, a cryptographic key may be decoded, it impersonates after authentication, and it cannot communicate between IC cards while ** is possible for after authentication.

[0036] Since the cryptographic key is changed for every communication link, decode of a cryptographic key becomes difficult, but it will become still more complicated constituting it, if it a configuration not only becomes complicated, but is combined with one of the above-mentioned authentication approaches, since the technique proposed by JP,2-195378,A omits authentication. Moreover, since the configuration and signal processing of an IC card and an IC card terminal are almost the same, although the communication link between IC cards is possible, in order to attest, when it combines with one of the above-mentioned authentication approaches, the communication link between IC cards will be impossible.
[0037] Then, this invention aims at offering the information correspondence procedure and equipment which can also prevent the malfeasance after authentication depended for impersonating, and can perform not only the communication link with an IC card and an IC card terminal but the communication link between IC cards while it prevents decode of a cryptographic key with an easy configuration.

[Translation done.]

* NOTICES *

MEANS

[Means for Solving the Problem] In order to attain the purpose mentioned above, in invention of claim 1 In the information correspondence procedure which communicates by repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment In case the 1st information over said 2nd equipment is transmitted from said 1st equipment, while generating the 1st random number with said 1st equipment Compound the 1st generated this random number and this 1st information, and it considers as the 1st synthetic information. this -- said 2nd equipment which enciphered the 1st synthetic information, transmitted to said 2nd equipment as 1st encryption information, and received said 1st encryption information from said 1st equipment It separates into said the 1st information and said 1st random number, after decrypting the 1st this encryption information which received. In case processing to said 1st information is performed and the 2nd information over said 1st equipment is transmitted from said 2nd equipment, while generating the 2nd random number with said 2nd equipment Compound the 2nd generated this random number, this 2nd information, and said 1st separated random number, and it considers as the 2nd synthetic information. this -- said 1st equipment which enciphered the 2nd synthetic information, transmitted to said 1st equipment as 2nd encryption information, and received the 2nd encryption information from said 2nd equipment It separates into said the 2nd information, said 2nd random number, and said 1st random number, after decrypting the 2nd this encryption information which received. When the 1st separated this random number is compared with said 1st generated random number and said 1st separated random number and said 1st generated random number are in agreement with this comparison, attest said 2nd equipment and processing to said 2nd information is performed. In case the 3rd information over said 2nd equipment is transmitted from said 1st equipment, while generating the 3rd random number with said 1st equipment Compound the 3rd generated this random number, this 3rd information, and said 2nd separated random number, and it considers as the 3rd synthetic information. this -- said 2nd equipment which enciphered the 3rd synthetic information, transmitted to said 2nd equipment as 3rd encryption information, and received the 3rd encryption information from said 1st equipment It separates into said the 3rd information, said 3rd random number, and said 2nd random number, after decrypting the 3rd this encryption information which received. When the 2nd separated this random number is compared with said 2nd generated random number and said 2nd separated random number and said 2nd generated random number are in agreement with this comparison, attest said 1st equipment and processing to said 3rd information is performed. It is characterized by repeating the above-mentioned processing until transmission and reception of the information between said 1st equipment and said 2nd equipment are completed.

[0039] Moreover, in invention of claim 2, it is characterized by being carried out using a cryptographic key with same the encryption and the decryption which said 1st equipment performs, encryption which said 2nd equipment performs, and decryption in invention of claim 1.

[0040] Moreover, in invention of claim 3, in invention of claim 1, said 1st equipment is an IC card and said 2nd equipment is characterized by being said IC card and the IC card terminal which performs an informational communication link.

[0041] Moreover, in invention of claim 4, it is characterized by said the 1st equipment and said 2nd equipment being an IC card in invention of claim 1.

[0042] Moreover, it sets to the information correspondence procedure which communicates in invention

of claim 5 by repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment. In case the 1st information over said 2nd equipment is transmitted from said 1st equipment, while generating the 1st random number with said 1st equipment Compound the 1st encryption information and said 1st generated random number, and it transmits to said 2nd equipment as the 1st transmit information. this 1st information -- enciphering -- the 1st encryption information -- carrying out -- this -- Said 2nd equipment which received said 1st transmit information from said 1st equipment After dividing the 1st this transmit information which received into said 1st random number and said 1st encryption information, this, while generating the 2nd random number with said 2nd equipment, in case the 1st encryption information is decrypted to said 1st information, processing to this 1st information is performed and the 2nd information over said 1st equipment is transmitted from said 2nd equipment Compound this 2nd information and said 1st separated random number, and it considers as the 2nd synthetic information. Compound the 2nd encryption information and said 2nd generated random number, and it transmits to said 1st equipment as the 2nd transmit information. this -- the 2nd synthetic information -- enciphering -- the 2nd encryption information -- carrying out -- this -- Said 1st equipment which received the 2nd transmit information from said 2nd equipment After dividing the 2nd this transmit information which received into said 2nd random number and said 2nd encryption information, Decrypt the 2nd encryption information to said 2nd synthetic information, and the 2nd this decrypted synthetic information is divided into said the 1st random number and said 2nd information. this -- When the 1st separated this random number is compared with said 1st generated random number and said 1st separated random number and said 1st generated random number are in agreement with this comparison, attest said 2nd equipment and processing to said 2nd information is performed. In case the 3rd information over said 2nd equipment is transmitted from said 1st equipment, while generating the 3rd random number with said 1st equipment Compound this 3rd information and said 2nd separated random number, and it considers as the 3rd synthetic information. Compound the 3rd encryption information and said 3rd generated random number, and it transmits to said 2nd equipment as the 3rd transmit information. this -- the 3rd synthetic information -- enciphering -- the 3rd encryption information -- carrying out -- this -- Said 2nd equipment which received the 3rd transmit information from said 1st equipment After dividing the 3rd this transmit information which received into said 3rd random number and said 3rd encryption information, Decrypt the 3rd encryption information to said 3rd synthetic information, and the 3rd this decrypted synthetic information is divided into said the 2nd random number and said 3rd information. this -- When the 2nd separated this random number is compared with said 2nd generated random number and said 2nd separated random number and said 2nd generated random number are in agreement with this comparison, attest said 1st equipment and processing to said 3rd information is performed. It is characterized by repeating the above-mentioned processing until transmission and reception of the information between said 1st equipment and said 2nd equipment are completed.

[0043] Moreover, in invention of claim 6, it is characterized by being carried out using a cryptographic key with same the encryption and the decryption which said 1st equipment performs, encryption which said 2nd equipment performs, and decryption in invention of claim 5.

[0044] Moreover, in invention of claim 7, in invention of claim 5, said 1st equipment is an IC card and said 2nd equipment is characterized by being said IC card and the IC card terminal which performs an informational communication link.

[0045] Moreover, in invention of claim 8, it is characterized by said the 1st equipment and said 2nd equipment being an IC card in invention of claim 5.

[0046] In the information communication device which communicates in invention of claim 9 by repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment moreover, said 1st equipment The 1st information processing means, the 1st random-number-generation means, the 1st synthetic means, the 1st encryption means, the 1st decryption means, the 1st separation means, and the 1st comparison means are provided. Said 2nd equipment The 2nd information processing means, the 2nd random-number-generation means, the 2nd synthetic means, the 2nd encryption means, the 2nd decryption means, the 2nd separation means, and the 2nd comparison means are provided. When said 1st equipment transmits information to said 2nd equipment While outputting the information which said 1st information processing means transmits, said 1st random-number-generation means generates a random number. The random number which said 2nd

equipment contained in information just before said 1st separation means received from said 2nd equipment generated is separated and acquired. After compounding the information which said 1st information processing means outputted, the random number which said 1st random-number-generation means generated, and the random number which said 1st separation means acquired with said 1st synthetic means, When it enciphers with said 1st encryption means, it transmits as encryption information and said 2nd equipment transmits information to said 1st equipment While outputting the information which said 2nd information processing means transmits, said 2nd random-number-generation means generates a random number. The random number which said 1st equipment contained in information just before said 2nd separation means received from said 1st equipment generated is separated and acquired. After compounding the information which said 2nd information processing means outputted, the random number which said 2nd random-number-generation means generated, and the random number which said 2nd separation means acquired with said 2nd synthetic means, When it enciphers with said 2nd encryption means, it transmits as encryption information and said 1st equipment receives the encryption information from said 2nd equipment It separates into the information which said 2nd information processing means outputted with said 1st separation means, the random number which said 2nd random-number-generation means generated, and the random number which said 2nd separation means acquired, after decrypting the received this encryption information with said 1st decryption means. Said 1st comparison means compares the acquired this random number and the random number which said 1st random-number-generation means generated. The information which said 2nd information processing means separated with said 1st separation means when this comparison result was coincidence outputted is processed with said 1st information processing means. When said 2nd equipment receives the encryption information from said 1st equipment It separates into the information which said 1st information processing means outputted with said 2nd separation means, the random number which said 1st random-number-generation means generated, and the random number which said 1st separation means acquired, after decrypting the received this encryption information with said 2nd decryption means. It is characterized by processing the information which said 1st information processing means which compared the acquired this random number with the random number which said 2nd random-number-generation means generated with said 2nd comparison means, and was separated with said 2nd separation means when this comparison result was coincidence outputted with said 2nd information processing means.

[0047] moreover, in transmitting information to said 2nd equipment in invention of claim 9 in invention of claim 10 before said 1st equipment receives information from said 2nd equipment Said 1st synthetic means compounds only the information which said 1st information processing means outputted, and the random number which said 1st random-number-generation means generated. In transmitting information to said 1st equipment before said 2nd equipment receives information from said 1st equipment Said 2nd synthetic means compounds only the information which said 2nd information processing means outputted, and the random number which said 2nd random-number-generation means generated. When information is received from said 2nd equipment before said 1st equipment transmitted information to said 2nd equipment The information which said 2nd information processing means separated with said 1st separation means, without said 1st comparison means comparing a random number outputted is processed with said 1st information processing means. When information is received from said 1st equipment before said 2nd equipment transmitted information to said 1st equipment It is characterized by processing the information which said 1st information processing means separated with said 2nd separation means, without said 2nd comparison means comparing a random number outputted with said 2nd information processing means.

[0048] Moreover, in invention of claim 11, it is characterized by using a cryptographic key with same said 1st encryption means, said 2nd encryption means, said 1st decryption means, and said 2nd decryption means in invention of claims 9 or 10.

[0049] Moreover, in invention of claim 12, in invention of claims 9 or 10, said 1st equipment is an IC card and said 2nd equipment is characterized by being said IC card and the IC card terminal which performs an informational communication link.

[0050] Moreover, in invention of claim 13, it is characterized by said the 1st equipment and said 2nd equipment being an IC card in invention of claims 9 or 10.

[0051] In the information communication device which communicates in invention of claim 14 by

repeating informational transmission and reception the number of predetermined times between the 1st equipment and the 2nd equipment moreover, said 1st equipment The 1st information processing means, the 1st random-number-generation means, the 1st upper composition means, the 1st lower layer composition means, the 1st encryption means, the 1st decryption means, the 1st upper separation means, the 1st lower layer separation means, and the 1st comparison means are provided. Said 2nd equipment possesses the 2nd information processing means, the 2nd random-number-generation means, the 2nd upper composition means, the 2nd lower layer composition means, the 2nd encryption means, the 2nd decryption means, the 2nd upper separation means, the 2nd lower layer separation means, and the 2nd comparison means. When said 1st equipment transmits information to said 2nd equipment While outputting the information which said 1st information processing means transmits, said 1st random-number-generation means generates a random number. The random number which said 2nd equipment contained in information just before said 1st separation means received from said 2nd equipment generated is separated and acquired. After compounding the information which said 1st information processing means outputted, and the random number which said 1st separation means acquired with said 1st lower layer composition means, Encipher with said 1st encryption means, consider as encryption information, and it transmits as synthetic information which compounded this encryption information and the random number which said 1st random-number-generation means generated with said 1st upper composition means. When said 2nd equipment transmits information to said 1st equipment While outputting the information which said 2nd information processing means transmits, said 2nd random-number-generation means generates a random number. The random number which said 1st equipment contained in information just before said 2nd separation means received from said 1st equipment generated is separated and acquired. After compounding the information which said 2nd information processing means outputted, and the random number which said 2nd separation means acquired with said 2nd lower layer composition means, Encipher with said 2nd encryption means, consider as encryption information, and it transmits as synthetic information which compounded this encryption information and the random number which said 2nd random-number-generation means generated with said 2nd upper composition means. When said 1st equipment receives the synthetic information from said 2nd equipment After said 1st upper separation means separates the random number which said 2nd random-number-generation means generated from the received this synthetic information, It separates into the information which decrypted with said 1st decryption means and said 2nd information processing means outputted with said 1st separation means further, and the random number which said 2nd separation means acquired. Said 1st comparison means compares the acquired this random number and the random number which said 1st random-number-generation means generated. The information which said 2nd information processing means separated with said 1st separation means when this comparison result was coincidence outputted is processed with said 1st information processing means. When said 2nd equipment receives the synthetic information from said 1st equipment After said 2nd upper separation means separates the random number which said 1st random-number-generation means generated from the received this synthetic information, It separates into the information which decrypted with said 2nd decryption means and said 1st information processing means outputted with said 2nd separation means further, and the random number which said 1st separation means acquired. It is characterized by processing the information which said 1st information processing means which compared the acquired this random number with the random number which said 2nd random-number-generation means generated with said 2nd comparison means, and was separated with said 2nd separation means when this comparison result was coincidence outputted with said 2nd information processing means.

[0052] moreover, in transmitting information to said 2nd equipment in invention of claim 14 in invention of claim 15 before said 1st equipment receives information from said 2nd equipment Said 1st encryption means enciphers only the information which said 1st information processing means outputted. In transmitting information to said 1st equipment before said 2nd equipment receives information from said 1st equipment Said 2nd encryption means enciphers only the information which said 2nd information processing means outputted. When information is received from said 2nd equipment before said 1st equipment transmitted information to said 2nd equipment The information which said 2nd information processing means separated with said 1st separation means, without said 1st comparison means comparing a random number outputted is processed with said 1st information processing means. When

information is received from said 1st equipment before said 2nd equipment transmitted information to said 1st equipment It is characterized by processing the information which said 1st information processing means separated with said 2nd separation means, without said 2nd comparison means comparing a random number outputted with said 2nd information processing means.
[0053] Moreover, in invention of claim 16, it is characterized by using a cryptographic key with same said 1st encryption means, said 2nd encryption means, said 1st decryption means, and said 2nd decryption means in invention of claims 14 or 15.
[0054] Moreover, in invention of claim 17, in invention of claims 14 or 15, said 1st equipment is an IC card and said 2nd equipment is characterized by being said IC card and the IC card terminal which performs an informational communication link.
[0055] Moreover, in invention of claim 18, it is characterized by said the 1st equipment and said 2nd equipment being an IC card in invention of claims 14 or 15.
[0056]
[Embodiment of the Invention] Hereafter, the information correspondence procedure concerning this invention and one example of equipment are explained to a detail with reference to an accompanying drawing.
[0057] Drawing 1 is the block diagram showing the IC card structure of a system. In drawing 1 , the IC card terminal 1 possesses the random-number-generation means 11, a random number and a merge means 12, the encryption means 13, the comparison means 14, the data-processing means 15, the cryptographic key storing means 16, a random number and a data separation means 17, and the decryption means 18, and is constituted. IC card 2 possesses the random-number-generation means 21, a random number and a merge means 22, the encryption means 23, the comparison means 24, the data-processing means 25, the cryptographic key storing means 26, a random number and a data separation means 27, and the decryption means 28, and is constituted.
[0058] In the IC card terminal 1, the data-processing means 15 processes generating processing of the data which deliver and receive between IC cards 2, and ********** to IC card 2 etc., the random-number-generation means 11 generates the random number of arbitration, and a random number and the merge means 12 compound the random number which the random-number-generation means 11 generates, the data which the data-processing means 15 outputs. This composition may be compounded based on a predetermined regulation so that it may serve as encryption, but since encryption is performed in the latter part, the composition which is only connected extent is enough as it. The encryption means 13 performs encryption processing using the random number compounded with the random number and the merge means 12, and the cryptographic key in which data etc. are stored by the cryptographic key storing means 16. The decryption means 18 carries out decryption processing using the cryptographic key in which the cipher transmitted from IC card 2 is stored by the cryptographic key storing means 16, and a random number and the data separation means 17 divide into a random number and data the information decrypted with the decryption means 18. The comparison means 14 compares the random number which the random-number-generation means 11 generated with the random number which performed predetermined processing later mentioned by these random numbers, and when the same (it will become the same if the predetermined processing mentioned later is made justly), it operates so that IC card 2 may be attested and data processing may be permitted to the data-processing means 15.
[0059] In IC card 2, similarly, the data-processing means 25 processes generating processing of the data which deliver and receive between the IC card terminals 1, and ********** to the IC card terminal 1 etc., the random-number-generation means 21 generates the random number of arbitration, and a random number and the merge means 22 compound the random number which the random-number-generation means 21 generates, the data which the data-processing means 25 outputs. The encryption means 23 performs encryption processing using the random number compounded with the random number and the merge means 22, and the cryptographic key in which data etc. are stored by the cryptographic key storing means 26. The cryptographic key stored in the cryptographic key storing means 26 is the same as that of the cryptographic key which the cryptographic key storing means 16 of the IC card terminal 1 stores. The decryption means 28 carries out decryption processing using the cryptographic key in which the cipher transmitted from the IC card terminal 1 is stored by the cryptographic key storing means 26, and a random number and the data separation means 27 divide into

a random number and data the information decrypted with the decryption means 28. The comparison means 24 compares the random number which the random-number-generation means 21 generated with the random number which performed predetermined processing later mentioned by these random numbers, and when the same, it operates so that the IC card terminal 1 may be attested and data processing may be permitted to the data-processing means 25.
[0060] Drawing 2 is drawing having shown actuation of IC card system shown in drawing 1 , and the flow of a signal.
[0061] First, if a user inserts IC card 2 in the IC card terminal 1 and both are connected electrically, the IC card terminal 1 will generate a random number R1 with the random-number-generation means 11, and will encipher a random number R1 with the encryption means 13 (step 51). At this time, after a random number R1 is compounded with the random-number demand which is a random-number-generation demand which receives to IC card 2 which the data-processing means 15 outputted with the random number and the merge means 12, it is enciphered using the cryptographic key stored in the cryptographic key storing means 16 with the encryption means 13.
[0062] The random number R1 and the random-number demand K (the random-number demand, R1) which were enciphered are sent out to IC card 2 (step 52), in IC card 2, are decrypted using the cryptographic key in which this is stored by the cryptographic key storing means 26 with the decryption means 28, and process received data with the data-processing means 25 through a random number and the data separation means 27 (step 53).
[0063] Next, based on the processing result of received data (based on a demand of the IC card terminal 1), the random-number-generation means 21 generates a random number R2 with the data-processing means 25. K (a response, R1R2) which compounded the reply signal over this, a random number R1, and a random-number demand with the random number and the merge means 22, and enciphered this using the cryptographic key storing means 16 with the encryption means 23 is sent out to (step 53) and the IC card terminal 1 (step 54).
[0064] The IC card terminal 1 which received K (a response, R1R2) decrypts this using the cryptographic key stored in the cryptographic key storing means 16 with the decryption means 18, separates a random number R1 with a random number and the data separation means 17, and passes delivery, and a reply signal and a random number R2 to the comparison means 14 to the data-processing means 15. With the comparison means 14, if the random number R1 separated with the random number and the data separation means 17 is compared with the random number R1 which the random-number-generation means 11 generated at step 51 and both are in agreement, IC card 2 will be attested and processing of data etc. will be permitted to the data-processing means 15. However, the authorization given to the data-processing means 15 here is only processing to the reply signal received with the random number R1 separated with the random number and the data separation means 17.
[0065] Attesting IC card 2, when the random-number-generation means 11 is in agreement at the random number R1 and step 51 which were separated with the random number and the data separation means 17 compared with the comparison means 14 That the demand and response to the IC card terminal 1 are transmitted with a random number R1 It is a reason for being impossible in addition to the partner who has the cryptographic key stored in the cryptographic key storing means 16. IC card terminal 1 self transmits the demand and response which are sent to coincidence even if it has answered a letter as it is in the random number R1 which the IC card terminal 1 enciphered and the inaccurate partner who does not have a cryptographic key temporarily transmitted, and an unjust demand is because it does not enter.
[0066] Next, a data-processing means 15 by which data processing was permitted Generate the access request to IC card 2, and this and the received random number R2 to a random number and the merge means 12 Delivery, A random number and the merge means 12 compound the random number R3 which this and the random-number-generation means 11 generated. To the encryption means 13 Delivery, It enciphers using the cryptographic key in which this is stored by the cryptographic key storing means 16, and the encryption means 13 is sent out to (step 55) and IC card 2 as K (an access request, R2R3) (step 56).
[0067] IC card 2 which received K (an access request, R2R3) decrypts this using the cryptographic key stored in the cryptographic key storing means 26 with the decryption means 28, separates a random number R2 with a random number and the data separation means 27, and passes delivery, and a reply

signal and a random number R3 to the comparison means 24 to the data-processing means 25. With the comparison means 24, if the random number R2 separated with the random number and the data separation means 27 is compared with the random number R2 which the random-number-generation means 21 generated at step 53 and both are in agreement, the IC card terminal 1 will be attested and processing of data etc. will be permitted to the data-processing means 25. The above-mentioned IC card terminal 1 of the reason for attesting the IC card terminal 1 by comparison with the comparison means 24 is the same as that of the reason for having attested IC card 2.

[0068] The data-processing means 25 will generate the access result to the IC card terminal 1, if data processing is permitted. The random number R4 with which, as for delivery, the random number, and the merge means 22, this and the random-number-generation means 21 generated this and the received random number R3 to the random number and the merge means 22 is compounded. To the encryption means 23 Delivery, It enciphers using the cryptographic key in which this is stored by the cryptographic key storing means 26, and the encryption means 23 is sent out to (step 57) and the IC card terminal 1 as K (an access result, R3R4) (step 58).

[0069] The IC card terminal 1 which received K (an access result, R3R4) decrypts this using the cryptographic key stored in the cryptographic key storing means 16 with the decryption means 18, separates a random number R3 with a random number and the data separation means 17, and passes delivery, and a reply signal and a random number R4 to the comparison means 14 to the data-processing means 15. With the comparison means 14, if the random number R3 separated with the random number and the data separation means 17 is compared with the random number R3 which the random-number-generation means 11 generated at step 55 and both are in agreement, IC card 2 will be attested and processing of data etc. will be permitted to the data-processing means 15. The data-processing means 15 will generate the directions or data M4 to IC card 2, if IC card 2 is attested by the comparison means 14. The random number R5 with which, as for delivery, the random number, and the merge means 12, this and the random-number-generation means 11 generated this and the received random number R4 to the random number and the merge means 12 is compounded. To the encryption means 13 Delivery, It enciphers using the cryptographic key in which this is stored by the cryptographic key storing means 16, and the encryption means 13 is sent out to (step 59) and IC card 2 as K (M4, R4R5) (step 60).

[0070] IC card 2 which received K (M4, R4R5) decrypts this using the cryptographic key stored in the cryptographic key storing means 26 with the decryption means 28, separates a random number R4 with a random number and the data separation means 27, and passes delivery, and a reply signal and a random number R5 to the comparison means 24 to the data-processing means 25. With the comparison means 24, if the random number R4 separated with the random number and the data separation means 27 is compared with the random number R4 which the random-number-generation means 21 generated at step 57 and both are in agreement, the IC card terminal 1 will be attested and processing of data etc. will be permitted to the data-processing means 25. The data-processing means 25 will generate the command or data M5 to the IC card terminal 1, if the IC card terminal 1 is attested by the comparison means 24. The random number R6 with which, as for delivery, the random number, and the merge means 22, this and the random-number-generation means 21 generated this and the received random number R5 to the random number and the merge means 22 is compounded. To the encryption means 23 Delivery, It enciphers using the cryptographic key in which this is stored by the cryptographic key storing means 26, and the encryption means 23 is sent out to (step 61) and the IC card terminal 1 as K (M5, R5R6) (step 62).

[0071] Like the following, the IC card terminal 1 processes, after attesting IC card 2 by the comparison of a random number R5 (step 63). Transmit K (M6, R6R7) to IC card 2 (step 64), and IC card 2 processes, after attesting the IC card terminal 1 by the comparison of a random number R6 (step 65). K (M7, R7R8) is transmitted to the IC card terminal 1 (step 66), and it repeats until a communication link ends this.

[0072] thus, the thing which the IC card terminal 1 and IC card 2 attest mutually for every communication link -- impersonating -- etc. -- injustice is prevented. Moreover, since the ciphers which have changed the cryptographic key as a result each time, that is, encipher the same plaintext (information which should communicate essentially) and are acquired since it is enciphering by compounding a random number to the information (a random-number demand, a response, an access

request, an access result, M1, M2 grade) which should communicate essentially differ each time for the compounded random number, it becomes difficult [decode of a cipher, or unjust acquisition of a cryptographic key] very much [them].

[0073] In addition, the same effectiveness can be acquired, even if it constitutes so that the random number transmitted first may be compounded with (R4 grade of 52 stepR1, 54 stepR2, 56 stepR3, and step 58), and other information enciphered without enciphering, for example, it may carry out like K (access request, R2)R3 at step 56 and it may transmit after being generated.

[0074] Next, the information correspondence procedure of IC card system concerning this invention and the 2nd example of equipment are explained.

[0075] Drawing 3 is the block diagram showing the IC card structure of a system in the case of performing the information communication link between IC cards. In drawing 3 IC card A2-1 the random-number-generation means 21-1, a random number and a merge means 22-1, the encryption means 23-1, the comparison means 24-1, the data-processing means 25-1, the cryptographic key storing means 26-1, a random number and a data separation means 27-1, and the decryption means 28-1 IC card B-2 -2 possesses the random-number-generation means 21-2, a random number and a merge means 22-2, the encryption means 23-2, the comparison means 24-2, the data-processing means 25-2, the cryptographic key storing means 26-2, a random number and a data separation means 27-2, and the decryption means 28-2, and is constituted. It connects through the IC card terminal 3.

[0076] In case data are communicated between this IC card A2-1 and IC card B-2 -2, since authentication and data communication are performed, explanation is omitted like the case where the communication link between the IC card terminal 1 explained in the 1st above-mentioned example and IC card 2 is performed.

[0077] Moreover, although IC card A2-1 and IC card B-2 -2 are connected through the IC card terminal 3, the IC card terminal 3 performs only actuation which passes the other party data, without processing the data which IC card A2-1 and IC card B-2 -2 sent out.

[0078] This IC card A2-1 and IC card B-2 -2 are the same configuration as IC card 2 explained in the above-mentioned example, and not only the data communication between IC cards but data communication with the IC card terminal 1 shown in drawing 1 is possible for them.

[Translation done.]

* NOTICES *

DESCRIPTION OF DRAWINGS

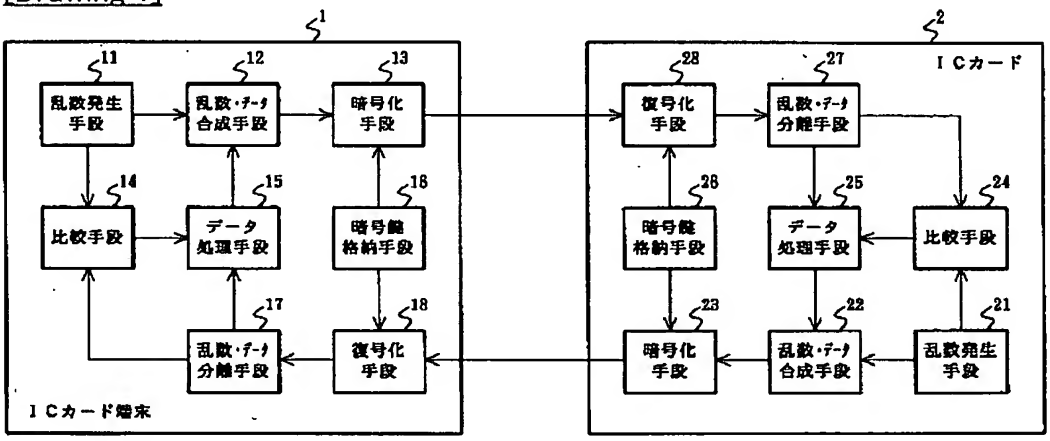
[Brief Description of the Drawings]
[Drawing 1] The block diagram showing the configuration of an IC card.
[Drawing 2] Drawing having shown actuation of IC card system shown in drawing 1 , and the flow of a signal.
[Drawing 3] The block diagram showing the IC card structure of a system in the case of performing an information communication link between IC cards.
[Drawing 4] Drawing having shown the flow of the block diagram having shown the 1st example of the conventional IC card system, and signal processing.
[Drawing 5] Drawing having shown the flow of the block diagram having shown the 2nd example of the conventional IC card system, and signal processing.
[Drawing 6] Drawing having shown the flow of the block diagram having shown the 3rd example of the conventional IC card system, and signal processing.
[Drawing 7] Drawing having shown the flow of the block diagram having shown the 4th example of the conventional IC card system, and signal processing.
[Drawing 8] Drawing having shown the flow of the block diagram having shown the 5th example of the conventional IC card system, and signal processing.
[Description of Notations]
1 IC Card Terminal
2 IC Card
3 IC Card Terminal
11 Random-Number-Generation Means
12 Random Number and Merge Means
13 Encryption Means
14 Comparison Means
15 Data-Processing Means
16 Cryptographic Key Storing Means
17 Random Number and Data Separation Means
18 Decryption Means
21, 21-1, 21-2 Random-number-generation means
22, 22-1, 22-2 A random number and merge means
23, 23-1, 23-2 Encryption means
24, 24-1, 24-2 Comparison means
25, 25-1, 25-2 Data-processing means
26, 26-1, 26-2 Cryptographic key storing means
27, 27-1, 27-2 A random number and data separation means
28, 28-1, 28-2 Decryption means

[Translation done.]

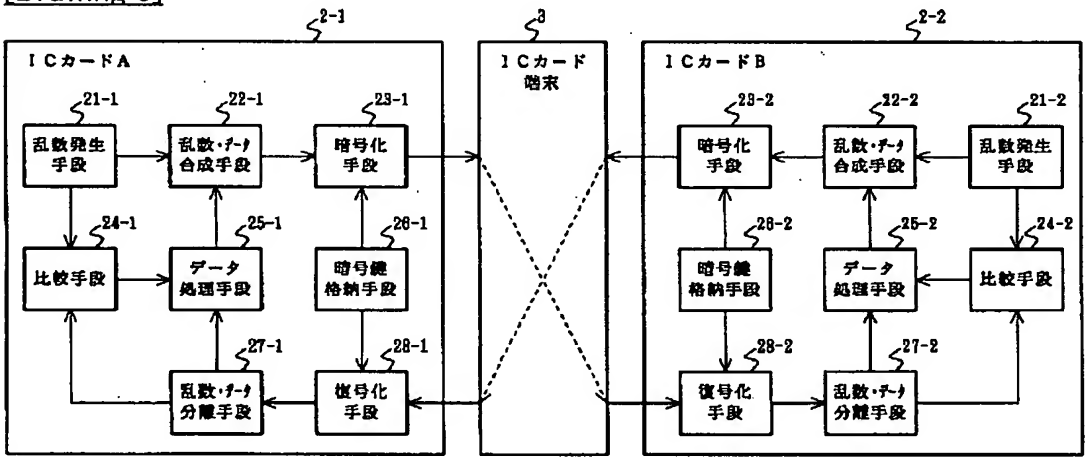
* NOTICES *

DRAWINGS

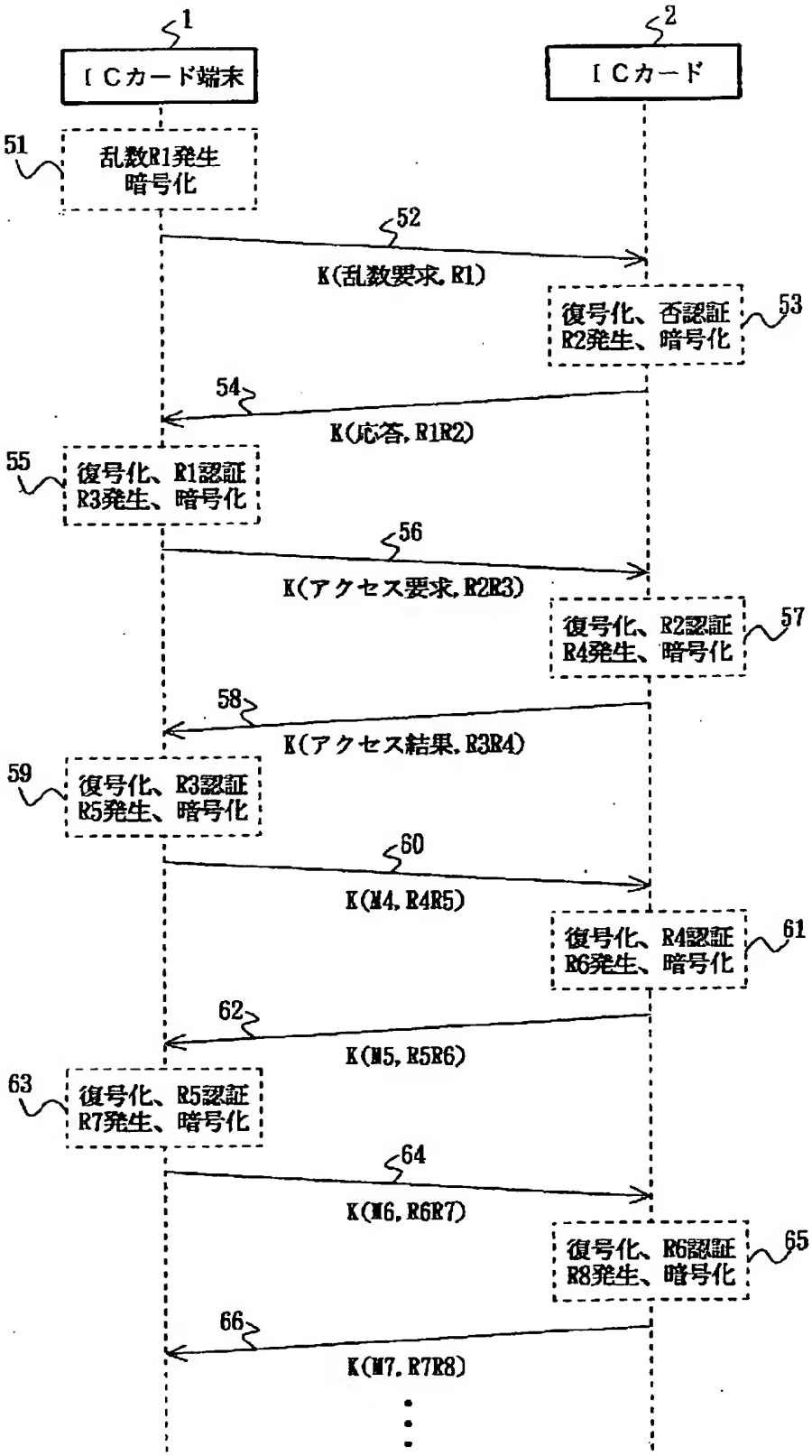
[Drawing 1]



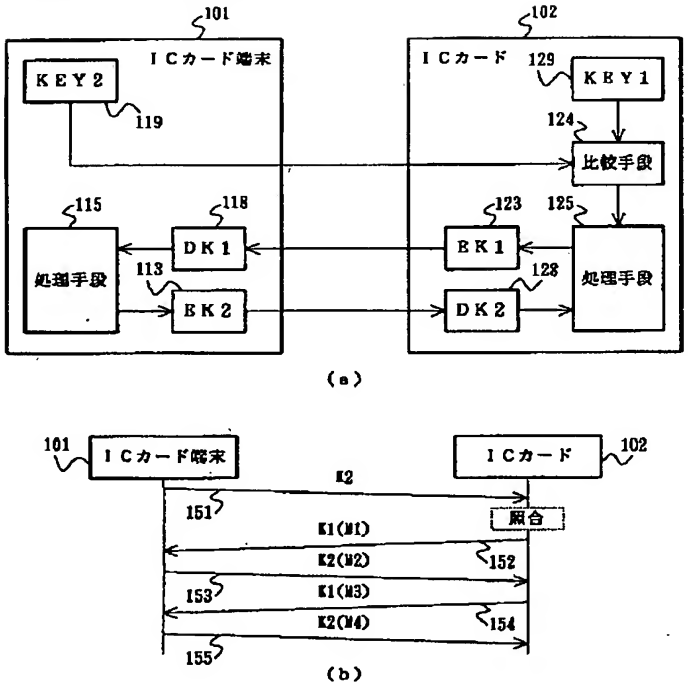
[Drawing 3]



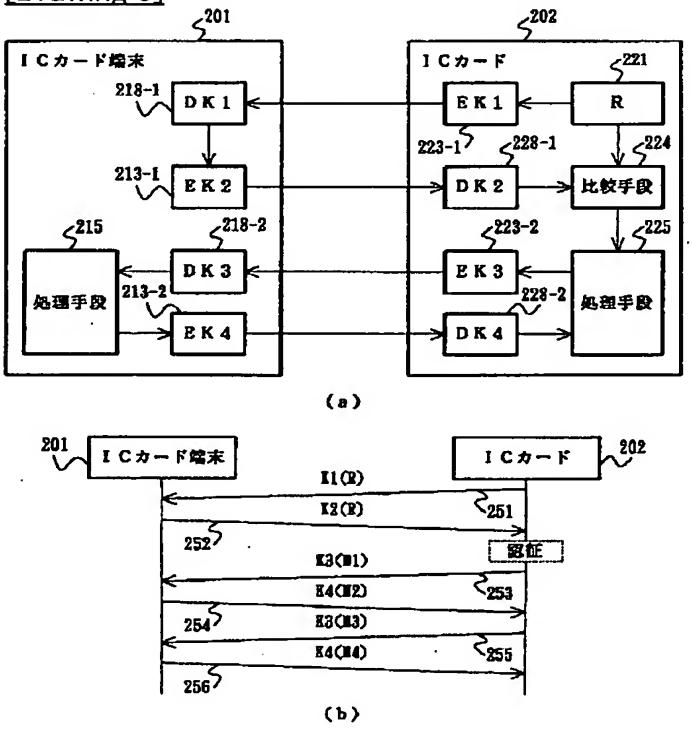
[Drawing 2]


1
ICカード端末
2
ICカード
51
乱数R1発生
暗号化
52
K(乱数要求, R1)
復号化、否認証
R2発生、暗号化
53
54
K(応答, R1R2)
55
復号化、R1認証
R3発生、暗号化
56
K(アクセス要求, R2R3)
復号化、R2認証
R4発生、暗号化
57
58
K(アクセス結果, R3R4)
59
復号化、R3認証
R5発生、暗号化
60
K(M4, R4R5)
復号化、R4認証
R6発生、暗号化
61
62
K(M5, R5R6)
63
復号化、R5認証
R7発生、暗号化
64
K(M6, R6R7)
復号化、R6認証
R8発生、暗号化
65
66
K(M7, R7R8)

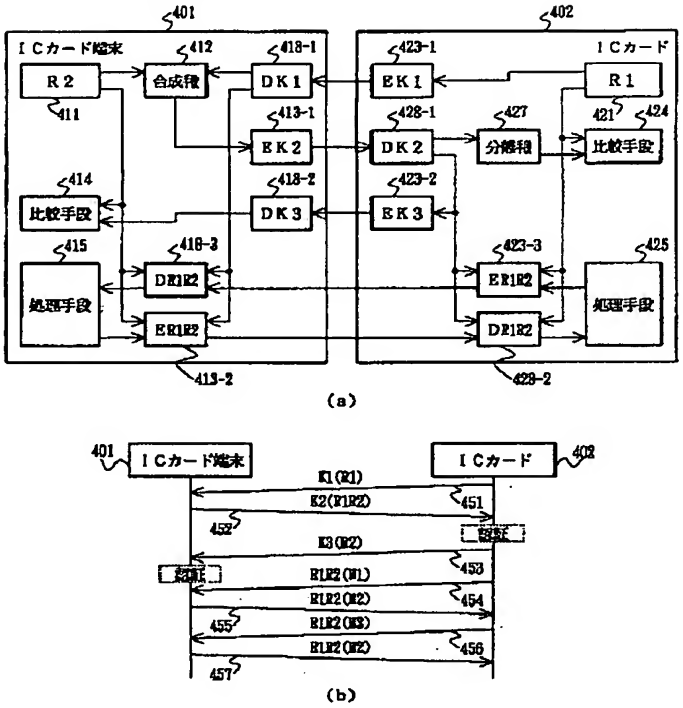
[Drawing 4]



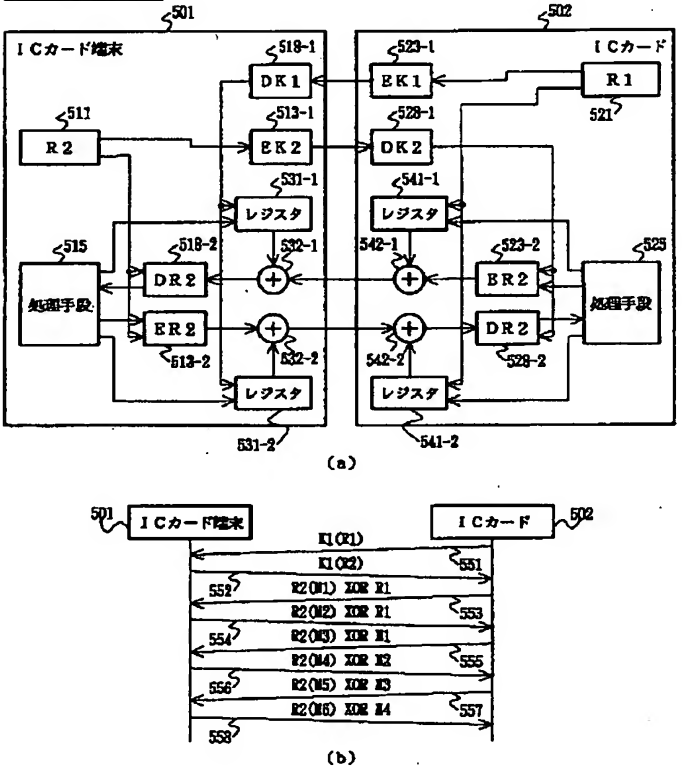
[Drawing 5]



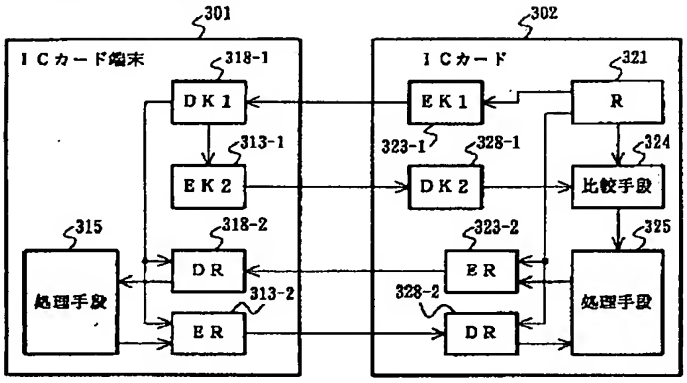
[Drawing 7]



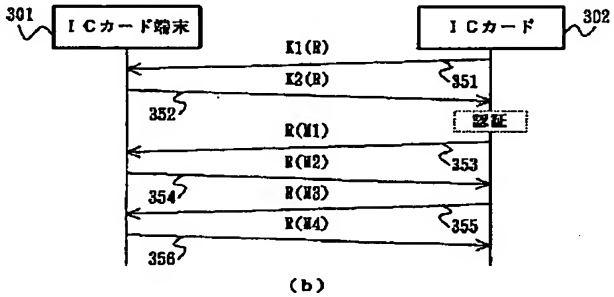
[Drawing 8]



[Drawing 6]



(a)



(b)

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－168461

(43)公開日　平成11年(1999)６月22日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ａ
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｔ
					Ｅ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ａ
		６６０			６６０Ａ

審査請求　未請求　請求項の数18　ＯＬ　（全 17 頁）　最終頁に続く

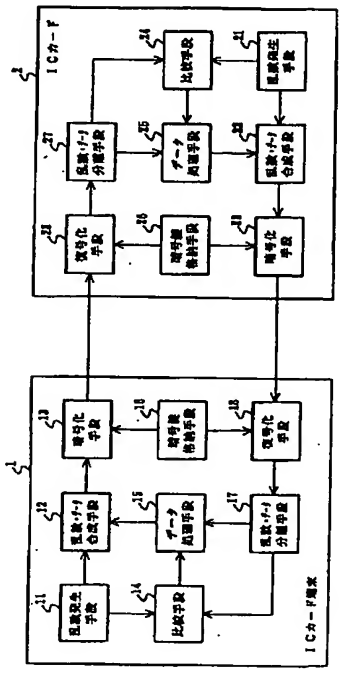
(21)出願番号　特願平9－334254

(22)出願日　平成９年(1997)12月４日

(71)出願人　000152859
株式会社日本コンラックス
東京都千代田区内幸町２丁目２番２号
(72)発明者　太田　通博
埼玉県坂戸市伊豆の山町55－２
(74)代理人　弁理士　木村　高久

(54)【発明の名称】　情報通信方法および装置

(57)【要約】
【課題】容易な構成で暗号鍵の解読を防止するとともに、認証後の成り済ましによる不正行為も防止し、かつ、ＩＣカードとＩＣカード端末との通信のみでなくＩＣカード間での通信を行うことのできる情報通信方法および装置を提供する。
【解決手段】ＩＣカード端末（１）とＩＣカード（２）が暗号化処理を施して情報の通信を行い、ＩＣカード端末（１）は、ＩＣカード（２）から受信した情報に合成されている乱数と、先にＩＣカード端末（１）からＩＣカード（２）へ送信した情報に合成した乱数とを比較手段（１４）で比較し、両者が等しかった場合にのみＩＣカードを認証してデータ処理手段（１５）に受信した情報の処理を許可し、ＩＣカード（２）も同様にＩＣカード端末（１）を認証してから受信した情報の処理を行う。



1

【特許請求の範囲】

【請求項１】　第１の装置と第２の装置との間で情報の送受を所定回数繰り返すことにより通信を行う情報通信方法において、

前記第１の装置から前記第２の装置に対する第１の情報を送信する際に、前記第１の装置で第１の乱数を発生するとともに、該発生した第１の乱数と該第１の情報とを合成して第１の合成情報とし、該第１の合成情報を暗号化して第１の暗号化情報として前記第２の装置へ送信し、

前記第１の装置から前記第１の暗号化情報を受信した前記第２の装置は、該受信した第１の暗号化情報を復号化した後、前記第１の情報と前記第１の乱数とに分離し、前記第１の情報に対する処理を行い、

前記第２の装置から前記第１の装置に対する第２の情報を送信する際に、前記第２の装置で第２の乱数を発生するとともに、該発生した第２の乱数と該第２の情報と前記分離した第１の乱数とを合成して第２の合成情報とし、該第２の合成情報を暗号化して第２の暗号化情報として前記第１の装置へ送信し、

前記第２の装置から第２の暗号化情報を受信した前記第１の装置は、該受信した第２の暗号化情報を復号化した後、前記第２の情報と前記第２の乱数と前記第１の乱数とに分離し、該分離した第１の乱数と前記発生した第１の乱数とを比較し、該比較により前記分離した第１の乱数と前記発生した第１の乱数とが一致した場合に前記第２の装置を認証して前記第２の情報に対する処理を行い、

前記第１の装置から前記第２の装置に対する第３の情報を送信する際に、前記第１の装置で第３の乱数を発生するとともに、該発生した第３の乱数と該第３の情報と前記分離した第２の乱数とを合成して第３の合成情報とし、該第３の合成情報を暗号化して第３の暗号化情報として前記第２の装置へ送信し、

前記第１の装置から第３の暗号化情報を受信した前記第２の装置は、該受信した第３の暗号化情報を復号化した後、前記第３の情報と前記第３の乱数と前記第２の乱数とに分離し、該分離した第２の乱数と前記発生した第２の乱数とを比較し、該比較により前記分離した第２の乱数と前記発生した第２の乱数とが一致した場合に前記第１の装置を認証して前記第３の情報に対する処理を行い、

前記第１の装置と前記第２の装置との間の情報の送受が終了するまで上記処理を繰り返すことを特徴とする情報通信方法。

【請求項２】　前記第１の装置が行う暗号化および復号化と前記第２の装置が行う暗号化および復号化とは、同一の暗号鍵を使用して行われることを特徴とする請求項１記載の情報通信方法。

【請求項３】　前記第１の装置は、

2

ＩＣカードであり、

前記第２の装置は、

前記ＩＣカードと情報の通信を行うＩＣカード端末であることを特徴とする請求項１記載の情報通信方法。

【請求項４】　前記第１の装置と前記第２の装置とは、ＩＣカードであることを特徴とする請求項１記載の情報通信方法。

【請求項５】　第１の装置と第２の装置との間で情報の送受を所定回数繰り返すことにより通信を行う情報通信方法において、

前記第１の装置から前記第２の装置に対する第１の情報を送信する際に、前記第１の装置で第１の乱数を発生するとともに、該第１の情報を暗号化して第１の暗号化情報とし、該第１の暗号化情報と前記発生した第１の乱数とを合成して第１の送信情報として前記第２の装置へ送信し、

前記第１の装置から前記第１の送信情報を受信した前記第２の装置は、該受信した第１の送信情報を前記第１の乱数と前記第１の暗号化情報とに分離した後、該第１の暗号化情報を前記第１の情報に復号化し、該第１の情報に対する処理を行い、

前記第２の装置から前記第１の装置に対する第２の情報を送信する際に、前記第２の装置で第２の乱数を発生するとともに、該第２の情報と前記分離した第１の乱数とを合成して第２の合成情報とし、該第２の合成情報を暗号化して第２の暗号化情報とし、該第２の暗号化情報と前記発生した第２の乱数とを合成して第２の送信情報として前記第１の装置へ送信し、

前記第２の装置から第２の送信情報を受信した前記第１の装置は、該受信した第２の送信情報を前記第２の乱数と前記第２の暗号化情報とに分離した後、該第２の暗号化情報を前記第２の合成情報に復号化し、該復号化した第２の合成情報を前記第１の乱数と前記第２の情報とに分離し、該分離した第１の乱数と前記発生した第１の乱数とを比較し、該比較により前記分離した第１の乱数と前記発生した第１の乱数とが一致した場合に前記第２の装置を認証して前記第２の情報に対する処理を行い、

前記第１の装置から前記第２の装置に対する第３の情報を送信する際に、前記第１の装置で第３の乱数を発生するとともに、該第３の情報と前記分離した第２の乱数とを合成して第３の合成情報とし、該第３の合成情報を暗号化して第３の暗号化情報とし、該第３の暗号化情報と前記発生した第３の乱数とを合成して第３の送信情報として前記第２の装置へ送信し、

前記第１の装置から第３の送信情報を受信した前記第２の装置は、該受信した第３の送信情報を前記第３の乱数と前記第３の暗号化情報とに分離した後、該第３の暗号化情報を前記第３の合成情報に復号化し、該復号化した第３の合成情報を前記第２の乱数と前記第３の情報とに分離し、該分離した第２の乱数と前記発生した第２の乱

数とを比較し、該比較により前記分離した第２の乱数と前記発生した第２の乱数とが一致した場合に前記第１の装置を認証して前記第３の情報に対する処理を行い、
前記第１の装置と前記第２の装置との間の情報の送受が終了するまで上記処理を繰り返すことを特徴とする情報通信方法。

【請求項６】　前記第１の装置が行う暗号化および復号化と前記第２の装置が行う暗号化および復号化とは、同一の暗号鍵を使用して行われることを特徴とする請求項５記載の情報通信方法。

【請求項７】　前記第１の装置は、
ＩＣカードであり、
前記第２の装置は、
前記ＩＣカードと情報の通信を行うＩＣカード端末であることを特徴とする請求項５記載の情報通信方法。

【請求項８】　前記第１の装置と前記第２の装置とは、
ＩＣカードであることを特徴とする請求項５記載の情報通信方法。

【請求項９】　第１の装置と第２の装置との間で情報の送受を所定回数繰り返すことにより通信を行う情報通信装置において、
前記第１の装置は、
第１の情報処理手段と第１の乱数発生手段と第１の合成手段と第１の暗号化手段と第１の復号化手段と第１の分離手段と第１の比較手段とを具備し、
前記第２の装置は、
第２の情報処理手段と第２の乱数発生手段と第２の合成手段と第２の暗号化手段と第２の復号化手段と第２の分離手段と第２の比較手段とを具備し、
前記第１の装置が前記第２の装置へ情報を送信する場合には、前記第１の情報処理手段が送信する情報を出力するとともに、前記第１の乱数発生手段が乱数を発生し、前記第１の分離手段が前記第２の装置から受信した直前の情報に含まれる前記第２の装置が発生した乱数を分離して取得し、前記第１の情報処理手段が出力した情報と前記第１の乱数発生手段が発生した乱数と前記第１の分離手段が取得した乱数とを前記第１の合成手段で合成した後、前記第１の暗号化手段で暗号化して暗号化情報として送信し、
前記第２の装置が前記第１の装置へ情報を送信する場合には、前記第２の情報処理手段が送信する情報を出力するとともに、前記第２の乱数発生手段が乱数を発生し、前記第２の分離手段が前記第１の装置から受信した直前の情報に含まれる前記第１の装置が発生した乱数を分離して取得し、前記第２の情報処理手段が出力した情報と前記第２の乱数発生手段が発生した乱数と前記第２の分離手段が取得した乱数とを前記第２の合成手段で合成した後、前記第２の暗号化手段で暗号化して暗号化情報として送信し、
前記第１の装置が前記第２の装置からの暗号化情報を受信した場合には、該受信した暗号化情報を前記第１の復号化手段で復号化した後、前記第１の分離手段で前記第２の情報処理手段が出力した情報と前記第２の乱数発生手段が発生した乱数と前記第２の分離手段が取得した乱数とに分離し、該取得した乱数と前記第１の乱数発生手段が発生した乱数とを前記第１の比較手段で比較し、該比較結果が一致であった場合に前記第１の分離手段で分離した前記第２の情報処理手段が出力した情報を前記第１の情報処理手段で処理し、
前記第２の装置が前記第１の装置からの暗号化情報を受信した場合には、該受信した暗号化情報を前記第２の復号化手段で復号化した後、前記第２の分離手段で前記第１の情報処理手段が出力した情報と前記第１の乱数発生手段が発生した乱数と前記第１の分離手段が取得した乱数とに分離し、該取得した乱数と前記第２の乱数発生手段が発生した乱数とを前記第２の比較手段で比較し、該比較結果が一致であった場合に前記第２の分離手段で分離した前記第１の情報処理手段が出力した情報を前記第２の情報処理手段で処理することを特徴とする情報通信装置。

【請求項１０】　前記第１の装置が前記第２の装置から情報を受信する前に前記第２の装置へ情報を送信する場合には、
前記第１の合成手段は、前記第１の情報処理手段が出力した情報と前記第１の乱数発生手段が発生した乱数とのみを合成し、
前記第２の装置が前記第１の装置から情報を受信する前に前記第１の装置へ情報を送信する場合には、
前記第２の合成手段は、前記第２の情報処理手段が出力した情報と前記第２の乱数発生手段が発生した乱数とのみを合成し、
前記第１の装置が前記第２の装置へ情報を送信する前に、前記第２の装置から情報を受信した場合には、
前記第１の比較手段が乱数の比較を行わずに前記第１の分離手段で分離した前記第２の情報処理手段が出力した情報を前記第１の情報処理手段で処理し、
前記第２の装置が前記第１の装置へ情報を送信する前に、前記第１の装置から情報を受信した場合には、
前記第２の比較手段が乱数の比較を行わずに前記第２の分離手段で分離した前記第１の情報処理手段が出力した情報を前記第２の情報処理手段で処理することを特徴とする請求項９記載の情報通信装置。

【請求項１１】　前記第１の暗号化手段と前記第２の暗号化手段と前記第１の復号化手段と前記第２の復号化手段とは、
同一の暗号鍵を使用することを特徴とする請求項９または１０記載の情報通信装置。

【請求項１２】　前記第１の装置は、
ＩＣカードであり、
前記第２の装置は、

前記ＩＣカードと情報の通信を行うＩＣカード端末であることを特徴とする請求項９または１０記載の情報通信装置。

【請求項１３】　前記第１の装置と前記第２の装置とは、

ＩＣカードであることを特徴とする請求項９または１０記載の情報通信装置。

【請求項１４】　第１の装置と第２の装置との間で情報の送受を所定回数繰り返すことにより通信を行う情報通信装置において、

前記第１の装置は、

第１の情報処理手段と第１の乱数発生手段と第１の上層合成手段と第１の下層合成手段と第１の暗号化手段と第１の復号化手段と第１の上層分離手段と第１の下層分離手段と第１の比較手段とを具備し、

前記第２の装置は、

第２の情報処理手段と第２の乱数発生手段と第２の上層合成手段と第２の下層合成手段と第２の暗号化手段と第２の復号化手段と第２の上層分離手段と第２の下層分離手段と第２の比較手段とを具備し、

前記第１の装置が前記第２の装置へ情報を送信する場合には、前記第１の情報処理手段が送信する情報を出力するとともに、前記第１の乱数発生手段が乱数を発生し、

前記第１の分離手段が前記第２の装置から受信した直前の情報に含まれる前記第２の装置が発生した乱数を分離して取得し、前記第１の情報処理手段が出力した情報と前記第１の分離手段が取得した乱数とを前記第１の下層合成手段で合成した後、前記第１の暗号化手段で暗号化して暗号化情報とし、該暗号化情報と前記第１の乱数発生手段が発生した乱数とを前記第１の上層合成手段で合成した合成情報として送信し、

前記第２の装置が前記第１の装置へ情報を送信する場合には、前記第２の情報処理手段が送信する情報を出力するとともに、前記第２の乱数発生手段が乱数を発生し、

前記第２の分離手段が前記第１の装置から受信した直前の情報に含まれる前記第１の装置が発生した乱数を分離して取得し、前記第２の情報処理手段が出力した情報と前記第２の分離手段が取得した乱数とを前記第２の下層合成手段で合成した後、前記第２の暗号化手段で暗号化して暗号化情報とし、該暗号化情報と前記第２の乱数発生手段が発生した乱数とを前記第２の上層合成手段で合成した合成情報として送信し、

前記第１の装置が前記第２の装置からの合成情報を受信した場合には、該受信した合成情報から前記第１の上層分離手段が前記第２の乱数発生手段が発生した乱数を分離した後、前記第１の復号化手段で復号化し、さらに前記第１の分離手段で前記第２の情報処理手段が出力した情報と前記第２の分離手段が取得した乱数とに分離し、該取得した乱数と前記第１の乱数発生手段が発生した乱数とを前記第１の比較手段で比較し、該比較結果が一致

であった場合に前記第１の分離手段で分離した前記第２の情報処理手段が出力した情報を前記第１の情報処理手段で処理し、

前記第２の装置が前記第１の装置からの合成情報を受信した場合には、該受信した合成情報から前記第２の上層分離手段が前記第１の乱数発生手段が発生した乱数を分離した後、前記第２の復号化手段で復号化し、さらに前記第２の分離手段で前記第１の情報処理手段が出力した情報と前記第１の分離手段が取得した乱数とに分離し、該取得した乱数と前記第２の乱数発生手段が発生した乱数とを前記第２の比較手段で比較し、該比較結果が一致であった場合に前記第２の分離手段で分離した前記第１の情報処理手段が出力した情報を前記第２の情報処理手段で処理することを特徴とする情報通信装置。

【請求項１５】　前記第１の装置が前記第２の装置から情報を受信する前に前記第２の装置へ情報を送信する場合には、

前記第１の暗号化手段は、前記第１の情報処理手段が出力した情報のみを暗号化し、

前記第２の装置が前記第１の装置から情報を受信する前に前記第１の装置へ情報を送信する場合には、

前記第２の暗号化手段は、前記第２の情報処理手段が出力した情報のみを暗号化し、

前記第１の装置が前記第２の装置へ情報を送信する前に、前記第２の装置から情報を受信した場合には、

前記第１の比較手段が乱数の比較を行わずに前記第１の分離手段で分離した前記第２の情報処理手段が出力した情報を前記第１の情報処理手段で処理し、

前記第２の装置が前記第１の装置へ情報を送信する前に、前記第１の装置から情報を受信した場合には、

前記第２の比較手段が乱数の比較を行わずに前記第２の分離手段で分離した前記第１の情報処理手段が出力した情報を前記第２の情報処理手段で処理することを特徴とする請求項１４記載の情報通信装置。

【請求項１６】　前記第１の暗号化手段と前記第２の暗号化手段と前記第１の復号化手段と前記第２の復号化手段とは、

同一の暗号鍵を使用することを特徴とする請求項１４または１５記載の情報通信装置。

【請求項１７】　前記第１の装置は、

ＩＣカードであり、

前記第２の装置は、

前記ＩＣカードと情報の通信を行うＩＣカード端末であることを特徴とする請求項１４または１５記載の情報通信装置。

【請求項１８】　前記第１の装置と前記第２の装置とは、

ＩＣカードであることを特徴とする請求項１４または１５記載の情報通信装置。

【発明の詳細な説明】

【０００１】
【発明の属する技術分野】この発明は、情報通信方法および装置に関し、特に、暗号鍵の漏洩を防止するとともにＩＣカードとＩＣカード端末間およびＩＣカード間で通信を行うことのできる情報通信方法および装置に関する。
【０００２】
【従来技術】ＩＣ（ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ：集積回路）を搭載したＩＣカードは、磁気カードと比較して情報の記憶容量が大きく、また、ＩＣカードの内部で演算等の処理を行わせることも可能であるため、その用途は多種多様である。
【０００３】この用途によっては、例えば金銭情報や機密情報を扱う場合等では、ＩＣカードとその周辺装置を含め、認証や情報の暗号化等の安全性の高い情報通信方法や装置の採用が重要な要件となる。
【０００４】ここで、ＩＣカードおよびその周辺装置における従来の情報通信方法および装置の一例を説明する。
【０００５】図４は、従来のＩＣカードシステムの一例を示したブロック図と信号の流れを示した図である。従来のＩＣカードシステムは、図４（ａ）に示すように、ＩＣカード端末１０１は秘密情報格納手段（ＫＥＹ２）１１９、処理手段１１５、暗号化手段（ＥＫ２）１１３、復号化手段（ＤＫ１）を具備し、ＩＣカード１０２は秘密情報格納手段（ＫＥＹ１）１２９、比較手段１２４、処理手段１２５、暗号化手段（ＥＫ１）１２３、復号化手段（ＤＫ２）１２８を具備して構成される。
【０００６】ここで、ＩＣカード端末１０１によりＩＣカード１０２に対する情報の書き込みや読み出しを行う場合の動作を説明する。
【０００７】ＩＣカード１０２がＩＣカード端末１０１に挿入されると、ＩＣカード端末１０１が秘密情報格納手段（ＫＥＹ２）１１９に格納されている秘密情報（ＫＥＹ２）をＩＣカード１０２へ送信する（ステップ１５１）。ＩＣカード１０２は秘密情報（ＫＥＹ２）を受信すると、これと秘密情報格納手段（ＫＥＹ１）１２９に格納されている秘密情報（ＫＥＹ１）を比較手段１２４で比較照合を行う。秘密情報（ＫＥＹ２）が秘密情報（ＫＥＹ１）と一致すれば、ＩＣカード１０２はＩＣカード端末１０１を正当なＩＣカード端末であると認証して、処理手段１２５に対して処理動作を許可する。動作が許可されると処理手段１２５は、ＩＣカード端末１０１の処理手段１１５とデータや命令等の通信を開始するが、通信を行う際には、処理手段１２５から送信されるデータ等（Ｍ１、Ｍ３）は、暗号化手段（ＥＫ１）１２３で暗号化されて送信され（ステップ１５２、１５４）、ＩＣカード端末１０１はこれを復号化手段（ＤＫ１）１１８で復号化して、処理手段１１５が処理を行う。また、処理手段１１５から送信されるデータ等（Ｍ２、Ｍ４）は、暗号化手段（ＥＫ２）１１３で暗号化されて送信され（ステップ１５３、１５５）、ＩＣカード１０２はこれを復号化手段（ＤＫ２）１２８で復号化して、処理手段１２５が処理を行う。
【０００８】このような処理を行うためには、暗号化手段（ＥＫ１）１２３と復号化手段（ＤＫ１）１１８が使用する暗号鍵が同一であり、暗号化手段（ＥＫ２）１１３と復号化手段（ＤＫ２）１２８が使用する暗号鍵が同一である必要があるが、４者の暗号鍵が同一であってもよい。また、秘密情報格納手段（ＫＥＹ２）１１９を暗証番号等の入力手段で構成し、ＩＣカード１０２がＩＣカード端末１０１を操作するユーザを認証するようにしてもよい。
【０００９】ところが、図４に示した構成においては、ＩＣカード端末１０１とＩＣカード１０２の間の通信を傍受することで、比較的容易に秘密情報を不正取得することが可能であり、秘密情報を取得すればＩＣカード１０２の情報の書き換えや偽造ＩＣカードを利用することが可能となるといった問題が生じる。
【００１０】また、暗号化した情報も常に同一の暗号鍵を用いて通信を行っているため、解読される可能性が高い。
【００１１】このような問題に対処するため、ＩＣカード端末とＩＣカードの間で秘密情報を通信せずに認証を行うとともに、暗号化した情報を容易に解読できないようにする技術が特開平２－３１２８９号公報や特開平２－３１２９０号公報、特開平２－４４３８９号公報、特開平２－１９５３７８号公報等で提案されている。
【００１２】特開平２－３１２８９号公報で提案されている技術は、図５（ａ）に示すように処理手段２１５、暗号化手段（ＥＫ２）２１３－１、暗号化手段（ＥＫ４）２１３－２、復号化手段（ＤＫ１）２１８－１、復号化手段（ＤＫ３）２１８－２を具備するＩＣカード端末２０１と、処理手段２２５、乱数発生手段（Ｒ）２２１、比較手段２２４、暗号化手段（ＥＫ１）２２３－１、暗号化手段（ＥＫ３）２２３－２、復号化手段（ＤＫ２）２２８－１、復号化手段（ＤＫ４）２２８－２を具備するＩＣカード２０２で構成される。
【００１３】このＩＣカードシステムは、図５（ｂ）に示すような流れで信号の授受を行う。まず、ＩＣカード２０２はＩＣカード端末２０１の認証を行うために、乱数発生手段（Ｒ）２２１で乱数（Ｒ）を発生し、これを暗号化手段（ＥＫ１）２２３－１で暗号化してＩＣカード端末２０１に送信し（ステップ２５１）、ＩＣカード端末２０１はこれを復号化手段（ＤＫ１）２１８－１で復号化し、復号化した乱数（Ｒ）を暗号化手段（ＥＫ２）２１３－１で暗号化してＩＣカード２０２へ送信する（ステップ２５２）。
【００１４】ＩＣカード２０２は受信した暗号情報を復号化手段（ＤＫ２）２２８－１で復号化して、この復号

化で得た乱数（Ｒ）と乱数発生手段（Ｒ）２２１が発生した乱数（Ｒ）を比較手段２２４で比較し、両者が一致すればＩＣカード端末２０１を認証して、処理手段２２５に動作許可を与える。

【００１５】これは、ＩＣカード２０２が発生して送信した乱数が正当な処理をされて返信されたことでＩＣカード端末２０１を認証するもので、暗号化手段（ＥＫ１）２２３－１と復号化手段（ＤＫ１）２１８－１が同一の暗号鍵を使用し、かつ、暗号化手段（ＥＫ２）２１３－１と復号化手段（ＤＫ２）２２８－１が同一の暗号鍵を使用している場合に成立する。ただし、この場合には暗号化手段（ＥＫ１）２２３－１と暗号化手段（ＥＫ２）２１３－１が使用する暗号鍵が同一であってはならない。

【００１６】ＩＣカード２０２がＩＣカード端末２０１を認証し、処理手段２２５の動作を許可すると、処理手段２２５は、ＩＣカード端末２０１の処理手段２１５とデータや命令等の通信を開始するが、通信を行う際には、処理手段２２５から送信されるデータ等（Ｍ１、Ｍ３）は、暗号化手段（ＥＫ３）２２３－２で暗号化されて送信され（ステップ２５３、２５５）、ＩＣカード端末２０１はこれを復号化手段（ＤＫ３）２１８－２で復号化して、処理手段２１５が処理を行う。また、処理手段２１５から送信されるデータ等（Ｍ２、Ｍ４）は、暗号化手段（ＥＫ４）２１３－２で暗号化されて送信され（ステップ２５４、２５６）、ＩＣカード２０２はこれを復号化手段（ＤＫ４）２２８－２で復号化して、処理手段２２５が処理を行う。

【００１７】この場合には、図４で説明したシステムとは異なり、秘密情報を直接送信することなく、認証時に使用する乱数を暗号鍵で暗号化することで、傍受で得られる情報を毎回異ならせ、暗号の解読は困難にしようとしている。

【００１８】特開平２－３１２９０号公報で提案されている技術は、図６（ａ）に示すように処理手段３１５、暗号化手段（ＥＫ２）３１３－１、暗号化手段（ＥＲ）３１３－２、復号化手段（ＤＫ１）３１８－１、復号化手段（ＤＲ）３１８－２を具備するＩＣカード端末３０１と、処理手段３２５、乱数発生手段（Ｒ）３２１、比較手段３２４、暗号化手段（ＥＫ１）３２３－１、暗号化手段（ＥＲ）３２３－２、復号化手段（ＤＫ２）３２８－１、復号化手段（ＤＲ）３２８－２を具備するＩＣカード３０２で構成される。

【００１９】このＩＣカードシステムは、図６（ｂ）に示すような流れで信号の授受を行うが、ステップ３５１、３５２で授受される信号によりＩＣカード３０２がＩＣカード端末３０１の認証を行う方法は、図５に示した場合と同様であるため説明は省略する。

【００２０】さて、ＩＣカード３０２がＩＣカード端末３０１を認証し、処理手段３２５の動作が許可されると、処理手段３２５は、ＩＣカード端末３０１の処理手段３１５とデータや命令等の通信を開始するが、通信を行う際には、処理手段３２５から送信されるデータ等（Ｍ１、Ｍ３）は、暗号化手段（ＥＲ）３２３－２で認証時に乱数発生手段（Ｒ）３２１が発生した乱数を暗号鍵として暗号化されて送信され（ステップ３５３、３５５）、ＩＣカード端末３０１はこれを復号化手段（ＤＲ）３１８－２で復号化して、処理手段３１５が処理を行う。また、処理手段３１５から送信されるデータ等（Ｍ２、Ｍ４）も、同様に暗号化手段（ＥＲ）３１３－２で認証時に乱数発生手段（Ｒ）３２１が発生した乱数（認証時に記憶）を暗号鍵として暗号化されて送信され（ステップ３５４、３５６）、ＩＣカード３０２はこれを復号化手段（ＤＲ）３２８－２で復号化して、処理手段３２５が処理を行う。

【００２１】この場合には、図５で説明したシステムに加え、データなどの通信を行う際の暗号化を認証時に発生した乱数を暗号鍵として使用することで、暗号鍵を毎回異ならせ、解読を困難にしようとしている。

【００２２】また、特開平２－４４３８９号公報で提案されている技術は、図７（ａ）に示すように処理手段４１５、乱数発生手段（Ｒ２）４１１、比較手段４１４、合成手段４１２、暗号化手段（ＥＫ２）４１３－１、暗号化手段（ＥＲ１Ｒ２）４１３－２、復号化手段（ＤＫ１）４１８－１、復号化手段（ＤＫ２）４１８－２、復号化手段（ＤＲ１Ｒ２）４１８－３を具備するＩＣカード端末４０１と、処理手段４２５、乱数発生手段（Ｒ１）４２１、比較手段４２４、分離手段４２７、暗号化手段（ＥＫ１）４２３－１、暗号化手段（ＥＫ３）４２３－２、暗号化手段（ＥＲ１Ｒ２）４２３－３、復号化手段（ＤＫ２）４２８－１、復号化手段（ＤＲ１Ｒ２）４２８－２を具備するＩＣカード４０２で構成される。

【００２３】このＩＣカードシステムは、図７（ｂ）に示すような流れで信号の授受を行う。まず、ＩＣカード４０２はＩＣカード端末４０１の認証を行うために、乱数発生手段（Ｒ１）４２１で乱数（Ｒ１）を発生し、これを暗号化手段（ＥＫ１）４２３－１で暗号化してＩＣカード端末４０１に送信する（ステップ４５１）。ＩＣカード端末４０１は受信した暗号化情報を復号化手段（ＤＫ１）４１８－１で復号化する一方で、ＩＣカード４０２の認証を行うために、乱数発生手段（Ｒ２）４１１で乱数（Ｒ２）を発生し、この乱数（Ｒ２）と復号化した乱数（Ｒ１）を合成手段４１２で合成し、これを暗号化手段（ＥＫ２）４１３－１で暗号化してＩＣカード４０２へ送信する（ステップ４５２）。

【００２４】ＩＣカード４０２は受信した暗号情報を復号化手段（ＤＫ２）４２８－１で復号化し、さらに分離手段４２７で乱数（Ｒ１）と乱数（Ｒ２）に分離する。分離された乱数（Ｒ１）は乱数発生手段（Ｒ１）４２１が発生した乱数（Ｒ１）と比較手段４２４で比較され、

両者が一致すればＩＣカード端末４０１を認証して、処理手段４２５に動作許可を与える。

【００２５】一方、分離手段４２７で分離された乱数（Ｒ２）は、暗号化手段（ＥＫ３）４２３－２で暗号化されてＩＣカード端末４０１へ送信され、ＩＣカード端末４０１は、受信した暗号情報を復号化手段（ＤＫ３）４１８－２で復号化し、復号化で得られた乱数（Ｒ２）と乱数発生手段（Ｒ２）４１１が発生した乱数（Ｒ２）を比較手段４１４で比較し、両者が一致すればＩＣカード４０２を認証して、処理手段４１５に動作許可を与える。

【００２６】ＩＣカード４０２がＩＣカード端末４０１を認証して処理手段４２５の動作を許可し、ＩＣカード端末４０１がＩＣカード４０２を認証して処理手段４１５の動作を許可すると、処理手段４１５と処理手段４２５は、相互にデータや命令等の通信を開始するが、通信を行う際には、処理手段４２５が送信するデータ等（Ｍ１、Ｍ３）は、暗号化手段（ＥＲ１Ｒ２）４２３－３で認証時に乱数発生手段（Ｒ１）４２１が発生した乱数（Ｒ１）と乱数発生手段（Ｒ２）４１１が発生した乱数（Ｒ２）を暗号鍵として暗号化されて送信され（ステップ４５４、４５６）、ＩＣカード端末４０１はこれを復号化手段（ＤＲ１Ｒ２）４１８－３で復号化して、処理手段４１５が処理を行う。また、処理手段４１５から送信されるデータ等（Ｍ２、Ｍ４）も、同様に暗号化手段（ＥＲ１Ｒ２）４１３－２で認証時に乱数発生手段（Ｒ１）４２１が発生した乱数（Ｒ１）と乱数発生手段（Ｒ２）４１１が発生した乱数（Ｒ２）を暗号鍵として暗号化されて送信され（ステップ４５５、４５７）、ＩＣカード４０２はこれを復号化手段（ＤＲ１Ｒ２）４２８－２で復号化して、処理手段４２５が処理を行う。

【００２７】このシステムは、図６で説明したシステムと比較して、ＩＣカードがＩＣカード端末を認証するだけでなく、ＩＣカード端末もＩＣカードを認証している点が異なっている。

【００２８】特開平２－１９５３７８号公報で提案されている技術は、図８（ａ）に示すように処理手段５１５、乱数発生手段（Ｒ２）５１１、暗号化手段（ＥＫ２）５１３－１、暗号化手段（ＥＲ２）５１３－２、復号化手段（ＤＫ１）５１８－１、復号化手段（ＤＲ２）５１８－２、レジスタ５３１－１、５３１－２、排他的論理和演算手段５３２－１、５３２－２を具備するＩＣカード端末５０１と、処理手段５２５、乱数発生手段（Ｒ１）５２１、暗号化手段（ＥＫ１）５２３－１、暗号化手段（ＥＲ２）５２３－２、復号化手段（ＤＫ２）５２８－１、復号化手段（ＤＲ２）５２８－２、レジスタ５４１－１、５４１－２、排他的論理和演算手段５４２－１、５４２－２を具備するＩＣカード５０２で構成される。

【００２９】このＩＣカードシステムは、図８（ｂ）に示すような流れで信号の授受を行うが、認証は特に行われてはいない。

【００３０】まず、データ等の通信に先立ち、ＩＣカード５０２が乱数発生手段（Ｒ１）５２１で乱数（Ｒ１）を発生して、これをレジスタ５４１－１、５４１－２へ格納するとともに暗号化手段（ＥＫ１）５２３－１で暗号化してＩＣカード端末５０１へ送信し（ステップ５５１）、ＩＣカード端末５０１はこれを復号化手段（ＤＫ１）５１８－１で復号化して得た乱数（Ｒ１）をレジスタ５３１－１、５３１－２へ格納する。また、ＩＣカード端末５０１は乱数発生手段（Ｒ２）５１１で乱数（Ｒ２）を発生し、これを暗号化手段（ＥＫ２）５１３－１で暗号化してＩＣカード５０２へ送信し（ステップ５５２）、ＩＣカード５０２は復号化手段（ＤＫ２）でこれを復号化して乱数（Ｒ２）を得る。

【００３１】このように相互に乱数（Ｒ１）と乱数（Ｒ２）を通知すると、ＩＣカード端末５０１とＩＣカード５０２は乱数（Ｒ１）と乱数（Ｒ２）を使用してデータや命令等の通信を開始するが、通信を行う際には、処理手段５２５から送信されるデータ等（Ｍ１、Ｍ３、Ｍ５）は、暗号化手段（ＥＲ２）５２３－２で乱数（Ｒ２）を暗号鍵として暗号化され、さらに排他的論理和演算手段５４２－１でレジスタ５４１－１に格納されている内容である乱数（Ｒ１）との排他的論理和が演算され、この演算結果が送信される（ステップ５５３）。ＩＣカード端末５０１は受信した暗号情報を排他的論理和演算手段５３２－１でレジスタ５３１－１に格納されている内容である乱数（Ｒ１）を利用して排他的論理和演算手段５４２－１での演算の逆演算を施し、これを復号化手段（ＤＲ２）５１８－２で乱数（Ｒ２）を暗号鍵として復号化して、処理手段５１５が処理を行う。また、レジスタ５３１－１、５４１－１に格納される内容は通信後にその通信内容であったデータ（Ｍ１）に変更され、次の通信ではデータ（Ｍ１）との排他的論理和が演算される（ステップ５５５）。

【００３２】同様に、処理手段５１５から送信されるデータ等（Ｍ２、Ｍ４、Ｍ６）も、暗号鍵に乱数（Ｒ２）を使用し、レジスタ５３１－１の格納内容との排他的論理和が演算されて送信される。

【００３３】このシステムは、排他的論理和の演算により通信毎に暗号鍵が変更されているのと同意となるため、暗号化情報の解読は困難である。

【００３４】

【発明が解決しようとする課題】ところが、特開平２－３１２８９号公報で提案されている技術では、認証を行った後は、常に同一の暗号鍵を使用して通信を行っているため、同じ暗号文が通信されることがあり、暗号鍵の解読が行われる可能性がある。例えば、アクセス要求やアクセス許可等の毎回通信される平文に対して同じ暗号鍵を使用すれば、常に同じ暗号文が通信されることにな

る。認証後の暗号鍵が解読されれば、ＩＣカードがＩＣカード端末を認証した後に通信に介入して、正当なＩＣカード端末に成り済ましてＩＣカードに対する不正なアクセスが可能となる。また、ＩＣカードとＩＣカード端末の構成や信号処理が同一でないため、この方法でＩＣカード端末を介さずに（何も処理をせずに）、ＩＣカード間で通信を行うことができない。

【００３５】特開平２－３１２９０号公報や特開平２－４４３８９号公報で提案されている技術では、使用毎（ＩＣカードがＩＣカード端末に挿入される毎）に暗号鍵が変更されるが、１回の使用については、認証後は同一の暗号鍵を使用するため、暗号鍵が解読される可能性もあり、認証後の成り済ましが可能であるとともにＩＣカード間で通信を行うことができない。

【００３６】特開平２－１９５３７８号公報で提案されている技術は、通信毎に暗号鍵を変更しているため暗号鍵の解読は困難となるが、構成が複雑となるばかりでなく、認証を行っていないため上述のいずれかの認証方法と組み合わせるとさらに構成が複雑となる。また、ＩＣカードとＩＣカード端末の構成や信号処理がほぼ同一であるため、ＩＣカード間の通信は可能であるが認証を行うため上述のいずれかの認証方法と組み合わせた場合には、ＩＣカード間の通信は不可能となってしまう。

【００３７】そこで、この発明は、容易な構成で暗号鍵の解読を防止するとともに、認証後の成り済ましによる不正行為も防止し、かつ、ＩＣカードとＩＣカード端末との通信のみでなくＩＣカード間での通信を行うことのできる情報通信方法および装置を提供することを目的とする。

【００３８】

【課題を解決するための手段】上述した目的を達成するため、請求項１の発明では、第１の装置と第２の装置との間で情報の送受を所定回数繰り返すことにより通信を行う情報通信方法において、前記第１の装置から前記第２の装置に対する第１の情報を送信する際に、前記第１の装置で第１の乱数を発生するとともに、該発生した第１の乱数と該第１の情報とを合成して第１の合成情報とし、該第１の合成情報を暗号化して第１の暗号化情報として前記第２の装置へ送信し、前記第１の装置から前記第１の暗号化情報を受信した前記第２の装置は、該受信した第１の暗号化情報を復号化した後、前記第１の情報と前記第１の乱数とに分離し、前記第１の情報に対する処理を行い、前記第２の装置から前記第１の装置に対する第２の情報を送信する際に、前記第２の装置で第２の乱数を発生するとともに、該発生した第２の乱数と該第２の情報と前記分離した第１の乱数とを合成して第２の合成情報とし、該第２の合成情報を暗号化して第２の暗号化情報として前記第１の装置へ送信し、前記第２の装置から第２の暗号化情報を受信した前記第１の装置は、該受信した第２の暗号化情報を復号化した後、前記第２の情報と前記第２の乱数と前記第１の乱数とに分離し、該分離した第１の乱数と前記発生した第１の乱数とを比較し、該比較により前記分離した第１の乱数と前記発生した第１の乱数とが一致した場合に前記第２の装置を認証して前記第２の情報に対する処理を行い、前記第１の装置から前記第２の装置に対する第３の情報を送信する際に、前記第１の装置で第３の乱数を発生するとともに、該発生した第３の乱数と該第３の情報と前記分離した第２の乱数とを合成して第３の合成情報とし、該第３の合成情報を暗号化して第３の暗号化情報として前記第２の装置へ送信し、前記第１の装置から第３の暗号化情報を受信した前記第２の装置は、該受信した第３の暗号化情報を復号化した後、前記第３の情報と前記第３の乱数と前記第２の乱数とに分離し、該分離した第２の乱数と前記発生した第２の乱数とを比較し、該比較により前記分離した第２の乱数と前記発生した第２の乱数とが一致した場合に前記第１の装置を認証して前記第３の情報に対する処理を行い、前記第１の装置と前記第２の装置との間の情報の送受が終了するまで上記処理を繰り返すことを特徴とする。

【００３９】また、請求項２の発明では、請求項１の発明において、前記第１の装置が行う暗号化および復号化と前記第２の装置が行う暗号化および復号化とは、同一の暗号鍵を使用して行われることを特徴とする。

【００４０】また、請求項３の発明では、請求項１の発明において、前記第１の装置は、ＩＣカードであり、前記第２の装置は、前記ＩＣカードと情報の通信を行うＩＣカード端末であることを特徴とする。

【００４１】また、請求項４の発明では、請求項１の発明において、前記第１の装置と前記第２の装置とは、ＩＣカードであることを特徴とする。

【００４２】また、請求項５の発明では、第１の装置と第２の装置との間で情報の送受を所定回数繰り返すことにより通信を行う情報通信方法において、前記第１の装置から前記第２の装置に対する第１の情報を送信する際に、前記第１の装置で第１の乱数を発生するとともに、該第１の情報を暗号化して第１の暗号化情報とし、該第１の暗号化情報と前記発生した第１の乱数とを合成して第１の送信情報として前記第２の装置へ送信し、前記第１の装置から前記第１の送信情報を受信した前記第２の装置は、該受信した第１の送信情報を前記第１の乱数と前記第１の暗号化情報とに分離した後、該第１の暗号化情報を前記第１の情報に復号化し、該第１の情報に対する処理を行い、前記第２の装置から前記第１の装置に対する第２の情報を送信する際に、前記第２の装置で第２の乱数を発生するとともに、該第２の情報と前記分離した第１の乱数とを合成して第２の合成情報とし、該第２の合成情報を暗号化して第２の暗号化情報とし、該第２の暗号化情報と前記発生した第２の乱数とを合成して第２の送信情報として前記第１の装置へ送信し、前記第２

の装置から第２の送信情報を受信した前記第１の装置は、該受信した第２の送信情報を前記第２の乱数と前記第２の暗号化情報とに分離した後、該第２の暗号化情報を前記第２の合成情報に復号化し、該復号化した第２の合成情報を前記第１の乱数と前記第２の情報とに分離し、該分離した第１の乱数と前記発生した第１の乱数とを比較し、該比較により前記分離した第１の乱数と前記発生した第１の乱数とが一致した場合に前記第２の装置を認証して前記第２の情報に対する処理を行い、前記第１の装置から前記第２の装置に対する第３の情報を送信する際に、前記第１の装置で第３の乱数を発生するとともに、該第３の情報と前記分離した第２の乱数とを合成して第３の合成情報とし、該第３の合成情報を暗号化して第３の暗号化情報とし、該第３の暗号化情報と前記発生した第３の乱数とを合成して第３の送信情報として前記第２の装置へ送信し、前記第１の装置から第３の送信情報を受信した前記第２の装置は、該受信した第３の送信情報を前記第３の乱数と前記第３の暗号化情報とに分離した後、該第３の暗号化情報を前記第３の合成情報に復号化し、該復号化した第３の合成情報を前記第２の乱数と前記第３の情報とに分離し、該分離した第２の乱数と前記発生した第２の乱数とを比較し、該比較により前記分離した第２の乱数と前記発生した第２の乱数とが一致した場合に前記第１の装置を認証して前記第３の情報に対する処理を行い、前記第１の装置と前記第２の装置との間の情報の送受が終了するまで上記処理を繰り返すことを特徴とする。

【００４３】また、請求項６の発明では、請求項５の発明において、前記第１の装置が行う暗号化および復号化と前記第２の装置が行う暗号化および復号化とは、同一の暗号鍵を使用して行われることを特徴とする。

【００４４】また、請求項７の発明では、請求項５の発明において、前記第１の装置は、ＩＣカードであり、前記第２の装置は、前記ＩＣカードと情報の通信を行うＩＣカード端末であることを特徴とする。

【００４５】また、請求項８の発明では、請求項５の発明において、前記第１の装置と前記第２の装置とは、ＩＣカードであることを特徴とする。

【００４６】また、請求項９の発明では、第１の装置と第２の装置との間で情報の送受を所定回数繰り返すことにより通信を行う情報通信装置において、前記第１の装置は、第１の情報処理手段と第１の乱数発生手段と第１の合成手段と第１の暗号化手段と第１の復号化手段と第１の分離手段と第１の比較手段とを具備し、前記第２の装置は、第２の情報処理手段と第２の乱数発生手段と第２の合成手段と第２の暗号化手段と第２の復号化手段と第２の分離手段と第２の比較手段とを具備し、前記第１の装置が前記第２の装置へ情報を送信する場合には、前記第１の情報処理手段が送信する情報を出力するとともに、前記第１の乱数発生手段が乱数を発生し、前記第１の分離手段が前記第２の装置から受信した直前の情報に含まれる前記第２の装置が発生した乱数を分離して取得し、前記第１の情報処理手段が出力した情報と前記第１の乱数発生手段が発生した乱数と前記第１の分離手段が取得した乱数とを前記第１の合成手段で合成した後、前記第１の暗号化手段で暗号化して暗号化情報として送信し、前記第２の装置が前記第１の装置へ情報を送信する場合には、前記第２の情報処理手段が送信する情報を出力するとともに、前記第２の乱数発生手段が乱数を発生し、前記第２の分離手段が前記第１の装置から受信した直前の情報に含まれる前記第１の装置が発生した乱数を分離して取得し、前記第２の情報処理手段が出力した情報と前記第２の乱数発生手段が発生した乱数と前記第２の分離手段が取得した乱数とを前記第２の合成手段で合成した後、前記第２の暗号化手段で暗号化して暗号化情報として送信し、前記第１の装置が前記第２の装置からの暗号化情報を受信した場合には、該受信した暗号化情報を前記第１の復号化手段で復号化した後、前記第１の分離手段で前記第２の情報処理手段が出力した情報と前記第２の乱数発生手段が発生した乱数と前記第２の分離手段が取得した乱数とに分離し、該取得した乱数と前記第１の乱数発生手段が発生した乱数とを前記第１の比較手段で比較し、該比較結果が一致であった場合に前記第１の分離手段で分離した前記第２の情報処理手段が出力した情報を前記第１の情報処理手段で処理し、前記第２の装置が前記第１の装置からの暗号化情報を受信した場合には、該受信した暗号化情報を前記第２の復号化手段で復号化した後、前記第２の分離手段で前記第１の情報処理手段が出力した情報と前記第１の乱数発生手段が発生した乱数と前記第１の分離手段が取得した乱数とに分離し、該取得した乱数と前記第２の乱数発生手段が発生した乱数とを前記第２の比較手段で比較し、該比較結果が一致であった場合に前記第２の分離手段で分離した前記第１の情報処理手段が出力した情報を前記第２の情報処理手段で処理することを特徴とする。

【００４７】また、請求項１０の発明では、請求項９の発明において、前記第１の装置が前記第２の装置から情報を受信する前に前記第２の装置へ情報を送信する場合には、前記第１の合成手段は、前記第１の情報処理手段が出力した情報と前記第１の乱数発生手段が発生した乱数とのみを合成し、前記第２の装置が前記第１の装置から情報を受信する前に前記第１の装置へ情報を送信する場合には、前記第２の合成手段は、前記第２の情報処理手段が出力した情報と前記第２の乱数発生手段が発生した乱数とのみを合成し、前記第１の装置が前記第２の装置へ情報を送信する前に、前記第２の装置から情報を受信した場合には、前記第１の比較手段が乱数の比較を行わずに前記第１の分離手段で分離した前記第２の情報処理手段が出力した情報を前記第１の情報処理手段で処理し、前記第２の装置が前記第１の装置へ情報を送信する

前に、前記第１の装置から情報を受信した場合には、前記第２の比較手段が乱数の比較を行わずに前記第２の分離手段で分離した前記第１の情報処理手段が出力した情報を前記第２の情報処理手段で処理することを特徴とする。

【００４８】また、請求項１１の発明では、請求項９または１０の発明において、前記第１の暗号化手段と前記第２の暗号化手段と前記第１の復号化手段と前記第２の復号化手段とは、同一の暗号鍵を使用することを特徴とする。

【００４９】また、請求項１２の発明では、請求項９または１０の発明において、前記第１の装置は、ＩＣカードであり、前記第２の装置は、前記ＩＣカードと情報の通信を行うＩＣカード端末であることを特徴とする。

【００５０】また、請求項１３の発明では、請求項９または１０の発明において、前記第１の装置と前記第２の装置とは、ＩＣカードであることを特徴とする。

【００５１】また、請求項１４の発明では、第１の装置と第２の装置との間で情報の送受を所定回数繰り返すことにより通信を行う情報通信装置において、前記第１の装置は、第１の情報処理手段と第１の乱数発生手段と第１の上層合成手段と第１の下層合成手段と第１の暗号化手段と第１の復号化手段と第１の上層分離手段と第１の下層分離手段と第１の比較手段とを具備し、前記第２の装置は、第２の情報処理手段と第２の乱数発生手段と第２の上層合成手段と第２の下層合成手段と第２の暗号化手段と第２の復号化手段と第２の上層分離手段と第２の下層分離手段と第２の比較手段とを具備し、前記第１の装置が前記第２の装置へ情報を送信する場合には、前記第１の情報処理手段が送信する情報を出力するとともに、前記第１の乱数発生手段が乱数を発生し、前記第１の分離手段が前記第２の装置から受信した直前の情報に含まれる前記第２の装置が発生した乱数を分離して取得し、前記第１の情報処理手段が出力した情報と前記第１の分離手段が取得した乱数とを前記第１の下層合成手段で合成した後、前記第１の暗号化手段で暗号化して暗号化情報とし、該暗号化情報と前記第１の乱数発生手段が発生した乱数とを前記第１の上層合成手段で合成した合成情報として送信し、前記第２の装置が前記第１の装置へ情報を送信する場合には、前記第２の情報処理手段が送信する情報を出力するとともに、前記第２の乱数発生手段が乱数を発生し、前記第２の分離手段が前記第１の装置から受信した直前の情報に含まれる前記第１の装置が発生した乱数を分離して取得し、前記第２の情報処理手段が出力した情報と前記第２の分離手段が取得した乱数とを前記第２の下層合成手段で合成した後、前記第２の暗号化手段で暗号化して暗号化情報とし、該暗号化情報と前記第２の乱数発生手段が発生した乱数とを前記第２の上層合成手段で合成した合成情報として送信し、前記第１の装置が前記第２の装置からの合成情報を受信した場合には、該受信した合成情報から前記第１の上層分離手段が前記第２の乱数発生手段が発生した乱数を分離した後、前記第１の復号化手段で復号化し、さらに前記第１の分離手段で前記第２の情報処理手段が出力した情報と前記第２の分離手段が取得した乱数とに分離し、該取得した乱数と前記第１の乱数発生手段が発生した乱数とを前記第１の比較手段で比較し、該比較結果が一致であった場合に前記第１の分離手段で分離した前記第２の情報処理手段が出力した情報を前記第１の情報処理手段で処理し、前記第２の装置が前記第１の装置からの合成情報を受信した場合には、該受信した合成情報から前記第２の上層分離手段が前記第１の乱数発生手段が発生した乱数を分離した後、前記第２の復号化手段で復号化し、さらに前記第２の分離手段で前記第１の情報処理手段が出力した情報と前記第１の分離手段が取得した乱数とに分離し、該取得した乱数と前記第２の乱数発生手段が発生した乱数とを前記第２の比較手段で比較し、該比較結果が一致であった場合に前記第２の分離手段で分離した前記第１の情報処理手段が出力した情報を前記第２の情報処理手段で処理することを特徴とする。

【００５２】また、請求項１５の発明では、請求項１４の発明において、前記第１の装置が前記第２の装置から情報を受信する前に前記第２の装置へ情報を送信する場合には、前記第１の暗号化手段は、前記第１の情報処理手段が出力した情報のみを暗号化し、前記第２の装置が前記第１の装置から情報を受信する前に前記第１の装置へ情報を送信する場合には、前記第２の暗号化手段は、前記第２の情報処理手段が出力した情報のみを暗号化し、前記第１の装置が前記第２の装置へ情報を送信する前に、前記第２の装置から情報を受信した場合には、前記第１の比較手段が乱数の比較を行わずに前記第１の分離手段で分離した前記第２の情報処理手段が出力した情報を前記第１の情報処理手段で処理し、前記第２の装置が前記第１の装置へ情報を送信する前に、前記第１の装置から情報を受信した場合には、前記第２の比較手段が乱数の比較を行わずに前記第２の分離手段で分離した前記第１の情報処理手段が出力した情報を前記第２の情報処理手段で処理することを特徴とする。

【００５３】また、請求項１６の発明では、請求項１４または１５の発明において、前記第１の暗号化手段と前記第２の暗号化手段と前記第１の復号化手段と前記第２の復号化手段とは、同一の暗号鍵を使用することを特徴とする。

【００５４】また、請求項１７の発明では、請求項１４または１５の発明において、前記第１の装置は、ＩＣカードであり、前記第２の装置は、前記ＩＣカードと情報の通信を行うＩＣカード端末であることを特徴とする。

【００５５】また、請求項１８の発明では、請求項１４または１５の発明において、前記第１の装置と前記第２の装置とは、ＩＣカードであることを特徴とする。

【００５６】
【発明の実施の形態】以下、この発明に係わる情報通信方法および装置の一実施例を添付図面を参照して詳細に説明する。
【００５７】図１は、ＩＣカードシステムの構成を示すブロック図である。図１において、ＩＣカード端末１は乱数発生手段１１、乱数・データ合成手段１２、暗号化手段１３、比較手段１４、データ処理手段１５、暗号鍵格納手段１６、乱数・データ分離手段１７、復号化手段１８を具備して構成され、ＩＣカード２は乱数発生手段２１、乱数・データ合成手段２２、暗号化手段２３、比較手段２４、データ処理手段２５、暗号鍵格納手段２６、乱数・データ分離手段２７、復号化手段２８を具備して構成される。
【００５８】ＩＣカード端末１において、データ処理手段１５はＩＣカード２との間で授受を行うデータの処理やＩＣカード２への動作指示等を発生させる等の処理を行い、乱数発生手段１１は任意の乱数を発生させ、乱数・データ合成手段１２は乱数発生手段１１が発生する乱数とデータ処理手段１５が出力するデータ等を合成する。この合成は、暗号化を兼ねるように所定の規則に基づいて合成してもよいが、後段で暗号化が行われるため単に連結する程度の合成で十分である。暗号化手段１３は乱数・データ合成手段１２で合成された乱数とデータ等を暗号鍵格納手段１６に格納されている暗号鍵を用いて暗号化処理を行う。復号化手段１８はＩＣカード２から送信される暗号文を暗号鍵格納手段１６に格納されている暗号鍵を用いて復号化処理し、乱数・データ分離手段１７は復号化手段１８で復号化された情報を乱数とデータに分離する。比較手段１４は乱数発生手段１１が発生した乱数と、この乱数に後述する所定の処理を施した乱数を比較し、同一であった場合（後述する所定の処理が正当になされれば同一となる）、ＩＣカード２を認証してデータ処理手段１５へデータ処理を許可するように動作する。
【００５９】ＩＣカード２においても同様に、データ処理手段２５はＩＣカード端末１との間で授受を行うデータの処理やＩＣカード端末１への動作指示等を発生させる等の処理を行い、乱数発生手段２１は任意の乱数を発生させ、乱数・データ合成手段２２は乱数発生手段２１が発生する乱数とデータ処理手段２５が出力するデータ等を合成する。暗号化手段２３は乱数・データ合成手段２２で合成された乱数とデータ等を暗号鍵格納手段２６に格納されている暗号鍵を用いて暗号化処理を行う。暗号鍵格納手段２６に格納されている暗号鍵は、ＩＣカード端末１の暗号鍵格納手段１６が格納している暗号鍵と同一である。復号化手段２８はＩＣカード端末１から送信される暗号文を暗号鍵格納手段２６に格納されている暗号鍵を用いて復号化処理し、乱数・データ分離手段２７は復号化手段２８で復号化された情報を乱数とデータに分離する。比較手段２４は乱数発生手段２１が発生した乱数と、この乱数に後述する所定の処理を施した乱数を比較し、同一であった場合、ＩＣカード端末１を認証してデータ処理手段２５へデータ処理を許可するように動作する。
【００６０】図２は、図１に示したＩＣカードシステムの動作および信号の流れを示した図である。
【００６１】まず、ユーザがＩＣカード２をＩＣカード端末１へ挿入し、両者が電気的に接続されると、ＩＣカード端末１は乱数発生手段１１で乱数Ｒ１を発生させ、暗号化手段１３で乱数Ｒ１を暗号化する（ステップ５１）。このとき、乱数Ｒ１は乱数・データ合成手段１２でデータ処理手段１５が出力したＩＣカード２へ対する乱数発生要求である乱数要求と合成されてから暗号化手段１３で暗号鍵格納手段１６に格納されている暗号鍵を用いて暗号化される。
【００６２】暗号化された乱数Ｒ１と乱数要求Ｋ（乱数要求，Ｒ１）はＩＣカード２へ送出され（ステップ５２）、ＩＣカード２ではこれを復号化手段２８で暗号鍵格納手段２６に格納されている暗号鍵を用いて復号化し、乱数・データ分離手段２７を介してデータ処理手段２５で受信データの処理を行う（ステップ５３）。
【００６３】次に、データ処理手段２５で受信データの処理結果に基づいて（ＩＣカード端末１の要求に基づいて）、乱数発生手段２１が乱数Ｒ２を発生して、これと乱数Ｒ１と乱数要求に対する応答信号を乱数・データ合成手段２２で合成し、これを暗号化手段２３で暗号鍵格納手段１６を用いて暗号化したＫ（応答，Ｒ１Ｒ２）を（ステップ５３）、ＩＣカード端末１に対して送出する（ステップ５４）。
【００６４】Ｋ（応答，Ｒ１Ｒ２）を受信したＩＣカード端末１は、復号化手段１８で暗号鍵格納手段１６に格納されている暗号鍵を用いてこれを復号化し、乱数・データ分離手段１７で乱数Ｒ１を分離して比較手段１４へ渡し、応答信号と乱数Ｒ２をデータ処理手段１５へ渡す。比較手段１４では、乱数・データ分離手段１７で分離された乱数Ｒ１とステップ５１で乱数発生手段１１が発生した乱数Ｒ１を比較し、両者が一致すればＩＣカード２を認証し、データ処理手段１５に対してデータ等の処理を許可する。ただし、ここでデータ処理手段１５に対して与えられる許可は乱数・データ分離手段１７で分離された乱数Ｒ１とともに受信された応答信号に対する処理のみである。
【００６５】比較手段１４で比較した乱数・データ分離手段１７で分離された乱数Ｒ１とステップ５１で乱数発生手段１１が一致した場合にＩＣカード２を認証するのは、ＩＣカード端末１への要求や応答が乱数Ｒ１とともに送信されることは、暗号鍵格納手段１６に格納された暗号鍵を有する相手以外には不可能であるといった理由であり、仮に暗号鍵を有さない不正な相手がＩＣカード

端末１が暗号化して送信した乱数Ｒ１をそのまま返信してきたとしても同時に送られる要求や応答はＩＣカード端末１自身が送信したものであり、不正な要求が入り込むことはないからである。

【００６６】次に、データ処理が許可されたデータ処理手段１５は、ＩＣカード２へのアクセス要求を発生し、これと受信した乱数Ｒ２を乱数・データ合成手段１２へ渡し、乱数・データ合成手段１２はこれと乱数発生手段１１が発生した乱数Ｒ３を合成して暗号化手段１３へ渡し、暗号化手段１３はこれを暗号鍵格納手段１６に格納されている暗号鍵を用いて暗号化してＫ（アクセス要求，Ｒ２Ｒ３）として（ステップ５５）、ＩＣカード２へ送出する（ステップ５６）。

【００６７】Ｋ（アクセス要求，Ｒ２Ｒ３）を受信したＩＣカード２は、復号化手段２８で暗号鍵格納手段２６に格納されている暗号鍵を用いてこれを復号化し、乱数・データ分離手段２７で乱数Ｒ２を分離して比較手段２４へ渡し、応答信号と乱数Ｒ３をデータ処理手段２５へ渡す。比較手段２４では、乱数・データ分離手段２７で分離された乱数Ｒ２とステップ５３で乱数発生手段２１が発生した乱数Ｒ２を比較し、両者が一致すればＩＣカード端末１を認証し、データ処理手段２５に対してデータ等の処理を許可する。比較手段２４での比較によりＩＣカード端末１を認証する理由は、上述のＩＣカード端末１がＩＣカード２を認証した理由と同じである。

【００６８】データ処理手段２５は、データ処理が許可されると、ＩＣカード端末１へのアクセス結果を発生し、これと受信した乱数Ｒ３を乱数・データ合成手段２２へ渡し、乱数・データ合成手段２２はこれと乱数発生手段２１が発生した乱数Ｒ４を合成して暗号化手段２３へ渡し、暗号化手段２３はこれを暗号鍵格納手段２６に格納されている暗号鍵を用いて暗号化してＫ（アクセス結果，Ｒ３Ｒ４）として（ステップ５７）、ＩＣカード端末１へ送出する（ステップ５８）。

【００６９】Ｋ（アクセス結果，Ｒ３Ｒ４）を受信したＩＣカード端末１は、復号化手段１８で暗号鍵格納手段１６に格納されている暗号鍵を用いてこれを復号化し、乱数・データ分離手段１７で乱数Ｒ３を分離して比較手段１４へ渡し、応答信号と乱数Ｒ４をデータ処理手段１５へ渡す。比較手段１４では、乱数・データ分離手段１７で分離された乱数Ｒ３とステップ５５で乱数発生手段１１が発生した乱数Ｒ３を比較し、両者が一致すればＩＣカード２を認証し、データ処理手段１５に対してデータ等の処理を許可する。データ処理手段１５は、比較手段１４によりＩＣカード２が認証されるとＩＣカード２への指示またはデータＭ４を発生し、これと受信した乱数Ｒ４を乱数・データ合成手段１２へ渡し、乱数・データ合成手段１２はこれと乱数発生手段１１が発生した乱数Ｒ５を合成して暗号化手段１３へ渡し、暗号化手段１３はこれを暗号鍵格納手段１６に格納されている暗号鍵を用いて暗号化してＫ（Ｍ４，Ｒ４Ｒ５）として（ステップ５９）、ＩＣカード２へ送出する（ステップ６０）。

【００７０】Ｋ（Ｍ４，Ｒ４Ｒ５）を受信したＩＣカード２は、復号化手段２８で暗号鍵格納手段２６に格納されている暗号鍵を用いてこれを復号化し、乱数・データ分離手段２７で乱数Ｒ４を分離して比較手段２４へ渡し、応答信号と乱数Ｒ５をデータ処理手段２５へ渡す。比較手段２４では、乱数・データ分離手段２７で分離された乱数Ｒ４とステップ５７で乱数発生手段２１が発生した乱数Ｒ４を比較し、両者が一致すればＩＣカード端末１を認証し、データ処理手段２５に対してデータ等の処理を許可する。データ処理手段２５は、比較手段２４によりＩＣカード端末１が認証されるとＩＣカード端末１への指令またはデータＭ５を発生し、これと受信した乱数Ｒ５を乱数・データ合成手段２２へ渡し、乱数・データ合成手段２２はこれと乱数発生手段２１が発生した乱数Ｒ６を合成して暗号化手段２３へ渡し、暗号化手段２３はこれを暗号鍵格納手段２６に格納されている暗号鍵を用いて暗号化してＫ（Ｍ５，Ｒ５Ｒ６）として（ステップ６１）、ＩＣカード端末１へ送出する（ステップ６２）。

【００７１】以下同様に、ＩＣカード端末１は乱数Ｒ５の比較でＩＣカード２を認証してから処理を行い（ステップ６３）、Ｋ（Ｍ６，Ｒ６Ｒ７）をＩＣカード２へ送信し（ステップ６４）、ＩＣカード２は乱数Ｒ６の比較でＩＣカード端末１を認証してから処理を行い（ステップ６５）、Ｋ（Ｍ７，Ｒ７Ｒ８）をＩＣカード端末１へ送信し（ステップ６６）、これを通信が終了するまで繰り返す。

【００７２】このように、通信毎にＩＣカード端末１とＩＣカード２が相互に認証を行うことで成り済まし等の不正を防止する。また、本来通信すべき情報（乱数要求、応答、アクセス要求、アクセス結果、Ｍ１、Ｍ２等）に乱数を合成して暗号化を行っているため、結果的には暗号鍵を毎回変更している、つまり、同じ平文（本来通信すべき情報）を暗号化して得られる暗号文は合成された乱数のために毎回異なるため、暗号文の解読や暗号鍵の不正取得が非常に困難となる。

【００７３】なお、発生されてから最初に送信される乱数は（ステップ５２のＲ１、ステップ５４のＲ２、ステップ５６のＲ３、ステップ５８のＲ４等）、暗号化せずに暗号化された他の情報と合成して、例えばステップ５６ではＫ（アクセス要求，Ｒ２）Ｒ３のようにして、送信するように構成しても同様の効果を得ることができる。

【００７４】次に、この発明に係わるＩＣカードシステムの情報通信方法および装置の第２の実施例を説明する。

【００７５】図３は、ＩＣカード間での情報通信を行う

場合のＩＣカードシステムの構成を示すブロック図である。図３において、ＩＣカードＡ２－１は乱数発生手段２１－１、乱数・データ合成手段２２－１、暗号化手段２３－１、比較手段２４－１、データ処理手段２５－１、暗号鍵格納手段２６－１、乱数・データ分離手段２７－１、復号化手段２８－１を、ＩＣカードＢ２－２は乱数発生手段２１－２、乱数・データ合成手段２２－２、暗号化手段２３－２、比較手段２４－２、データ処理手段２５－２、暗号鍵格納手段２６－２、乱数・データ分離手段２７－２、復号化手段２８－２を具備して構成され、ＩＣカード端末３を介して接続される。

【００７６】このＩＣカードＡ２－１とＩＣカードＢ２－２の間でデータの通信を行う際には、上述の第１の実施例で説明したＩＣカード端末１とＩＣカード２の間での通信を行う場合と同様に、認証およびデータ通信を行うので説明は省略する。

【００７７】また、ＩＣカードＡ２－１とＩＣカードＢ２－２はＩＣカード端末３を介して接続されるが、ＩＣカード端末３はＩＣカードＡ２－１およびＩＣカードＢ２－２が送出したデータの処理を行わずに相手方へデータを渡すだけの動作のみを行う。

【００７８】このＩＣカードＡ２－１とＩＣカードＢ２－２は、上述の実施例で説明したＩＣカード２と同様の構成であり、ＩＣカード間のデータ通信のみでなく、図１に示したＩＣカード端末１とのデータ通信も可能である。

【００７９】

【発明の効果】以上説明したように、この発明によれば、ＩＣカード端末とＩＣカードが暗号化処理を施して情報の通信を行い、ＩＣカード端末は、ＩＣカードから受信した情報に合成されている乱数が、先にＩＣカード端末からＩＣカードへ送信した情報に合成した乱数と等しかった場合にのみＩＣカードを認証して受信した情報の処理を行い、ＩＣカードも同様にＩＣカード端末を認証してから受信した情報の処理を行うように構成したので、盗聴等による暗号鍵の漏洩を防止できるとともに、「成り済まし」行為等の不正行為を防ぐこともできる。

【００８０】また、ＩＣカード端末とＩＣカードを同様の手段を具備して構成したため、ＩＣカードとＩＣカードの間でのデータ通信をデータ処理機構を有しないＩＣカード端末を介して行うこともできる。

【図面の簡単な説明】

【図１】ＩＣカードの構成を示すブロック図。

【図２】図１に示したＩＣカードシステムの動作および信号の流れを示した図。

【図３】ＩＣカード間で情報通信を行う場合のＩＣカードシステムの構成を示すブロック図。

【図４】従来のＩＣカードシステムの第１例を示したブロック図と信号処理の流れを示した図。

【図５】従来のＩＣカードシステムの第２例を示したブロック図と信号処理の流れを示した図。

【図６】従来のＩＣカードシステムの第３例を示したブロック図と信号処理の流れを示した図。

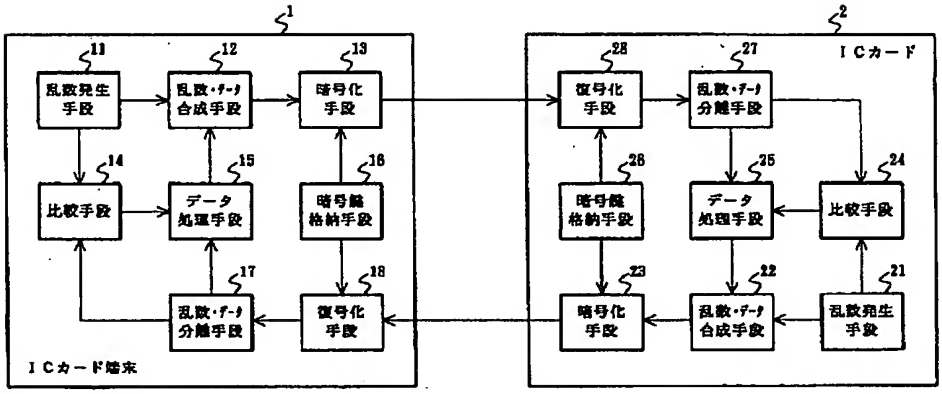
【図７】従来のＩＣカードシステムの第４例を示したブロック図と信号処理の流れを示した図。

【図８】従来のＩＣカードシステムの第５例を示したブロック図と信号処理の流れを示した図。

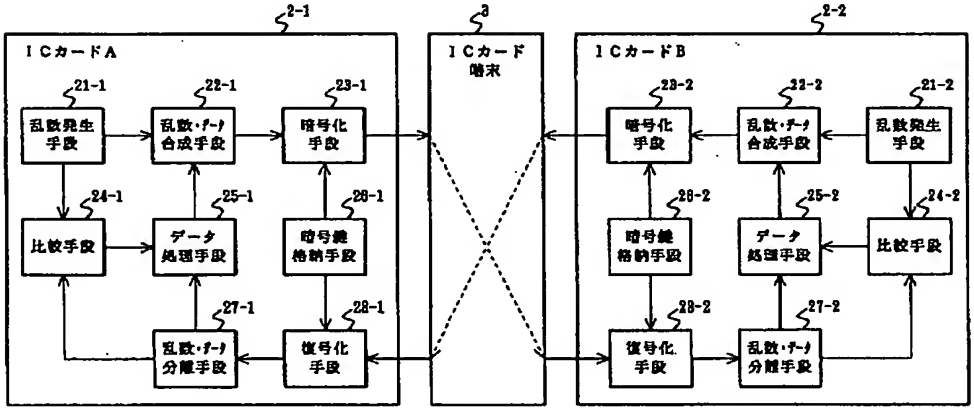
【符号の説明】

１　ＩＣカード端末
２　ＩＣカード
３　ＩＣカード端末
１１　乱数発生手段
１２　乱数・データ合成手段
１３　暗号化手段
１４　比較手段
１５　データ処理手段
１６　暗号鍵格納手段
１７　乱数・データ分離手段
１８　復号化手段
２１、２１－１、２１－２　乱数発生手段
２２、２２－１、２２－２　乱数・データ合成手段
２３、２３－１、２３－２　暗号化手段
２４、２４－１、２４－２　比較手段
２５、２５－１、２５－２　データ処理手段
２６、２６－１、２６－２　暗号鍵格納手段
２７、２７－１、２７－２　乱数・データ分離手段
２８、２８－１、２８－２　復号化手段

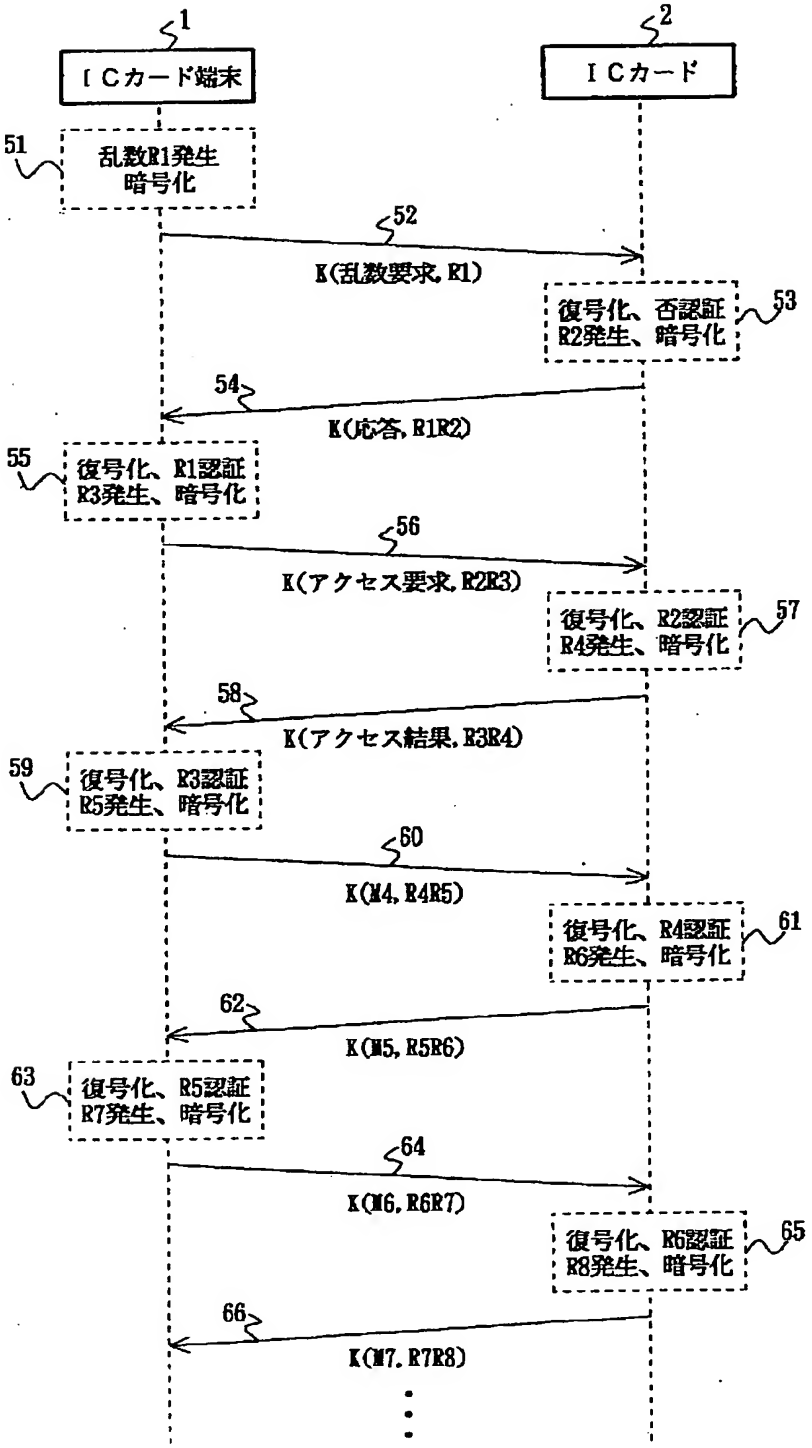
【図１】


1
11
乱数発生手段
12
乱数・データ合成手段
13
暗号化手段
14
比較手段
15
データ処理手段
16
暗号鍵格納手段
17
乱数・データ分離手段
18
復号化手段
ＩＣカード端末
2
ＩＣカード
28
復号化手段
27
乱数・データ分離手段
26
暗号鍵格納手段
25
データ処理手段
24
比較手段
23
暗号化手段
22
乱数・データ合成手段
21
乱数発生手段

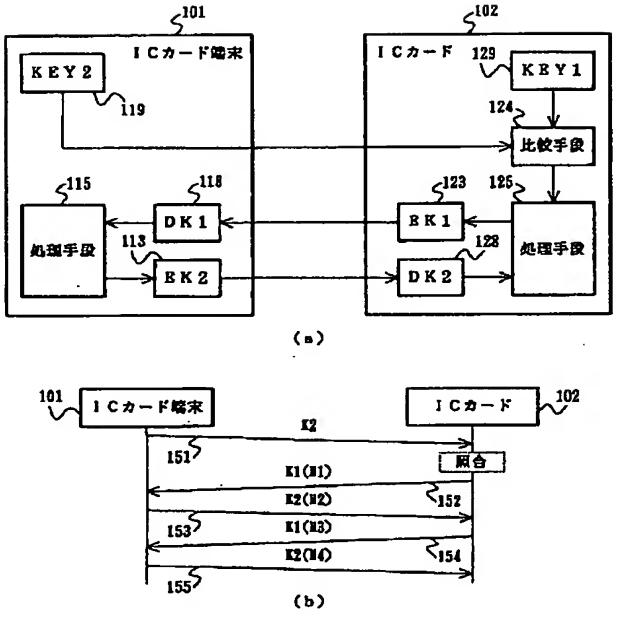
【図３】


2-1
ＩＣカードＡ
21-1
乱数発生手段
22-1
乱数・データ合成手段
23-1
暗号化手段
24-1
比較手段
25-1
データ処理手段
26-1
暗号鍵格納手段
27-1
乱数・データ分離手段
28-1
復号化手段
3
ＩＣカード端末
2-2
ＩＣカードＢ
23-2
暗号化手段
22-2
乱数・データ合成手段
21-2
乱数発生手段
26-2
暗号鍵格納手段
25-2
データ処理手段
24-2
比較手段
28-2
復号化手段
27-2
乱数・データ分離手段

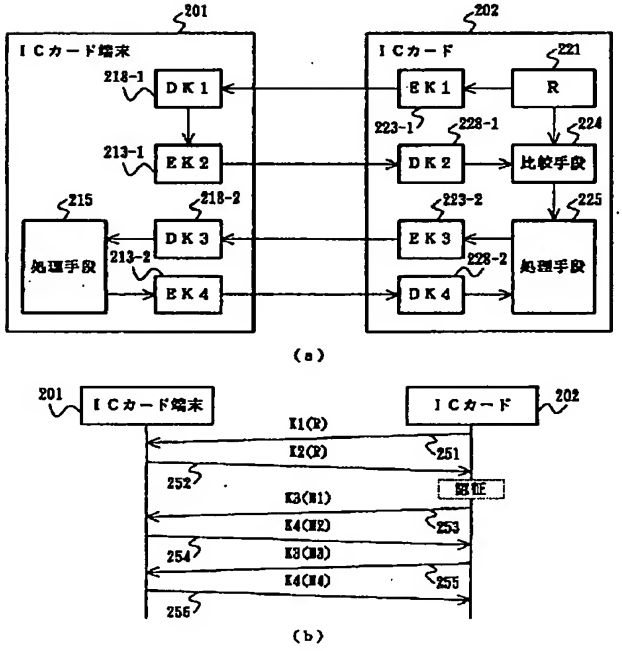
【図２】


1
ＩＣカード端末
2
ＩＣカード
51
乱数R1発生
暗号化
52
K(乱数要求, R1)
復号化、否認証
R2発生、暗号化
53
54
K(応答, R1R2)
55
復号化、R1認証
R3発生、暗号化
56
K(アクセス要求, R2R3)
復号化、R2認証
R4発生、暗号化
57
58
K(アクセス結果, R3R4)
59
復号化、R3認証
R5発生、暗号化
60
K(M4, R4R5)
復号化、R4認証
R6発生、暗号化
61
62
K(M5, R5R6)
63
復号化、R5認証
R7発生、暗号化
64
K(M6, R6R7)
復号化、R6認証
R8発生、暗号化
65
66
K(M7, R7R8)

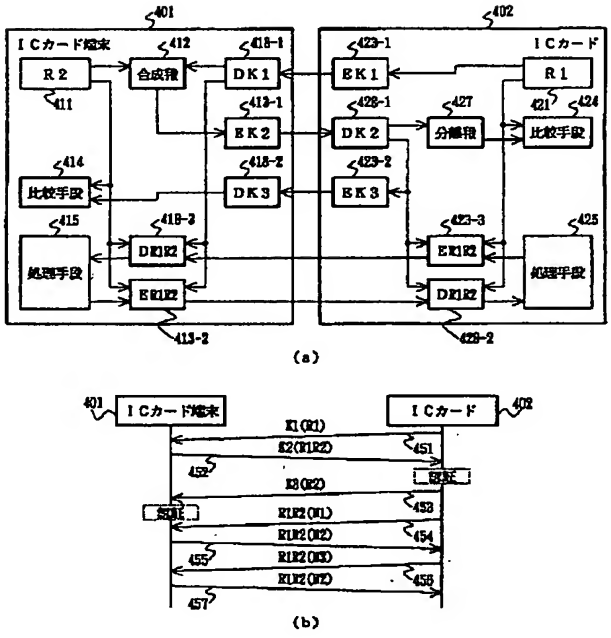
【図４】


101
ＩＣカード端末
ＫＥＹ２
119
115
処理手段
118
ＤＫ１
113
ＥＫ２
102
ＩＣカード
129
ＫＥＹ１
124
比較手段
123
ＥＫ１
125
処理手段
128
ＤＫ２
(a)
101
ＩＣカード端末
102
ＩＣカード
K2
151
照合
K1(N1)
K2(N2)
152
153
K1(N3)
K2(N4)
154
155
(b)

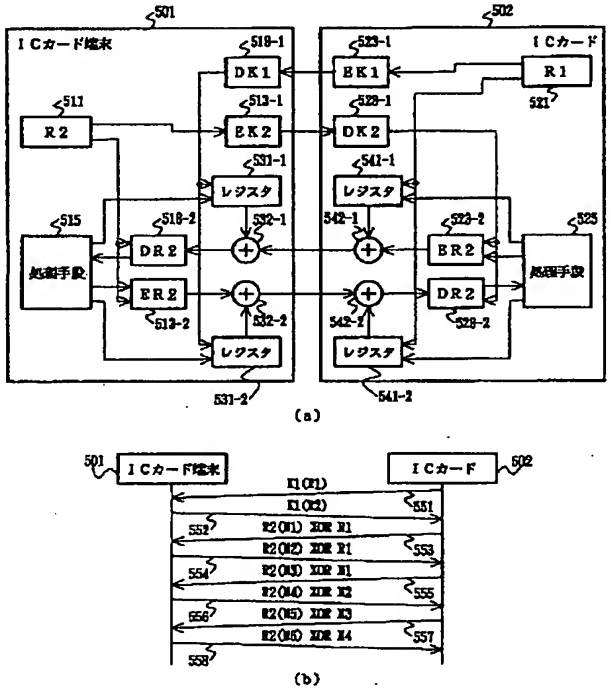
【図５】


201
ＩＣカード端末
218-1
ＤＫ１
213-1
ＥＫ２
215
処理手段
218-2
ＤＫ３
213-2
ＥＫ４
202
ＩＣカード
221
Ｒ
223-1
ＥＫ１
228-1
ＤＫ２
224
比較手段
223-2
ＥＫ３
225
処理手段
228-2
ＤＫ４
(a)
201
ＩＣカード端末
202
ＩＣカード
K1(R)
K2(R)
251
252
照合
K3(N1)
K4(N2)
253
254
K3(N3)
K4(N4)
255
256
(b)

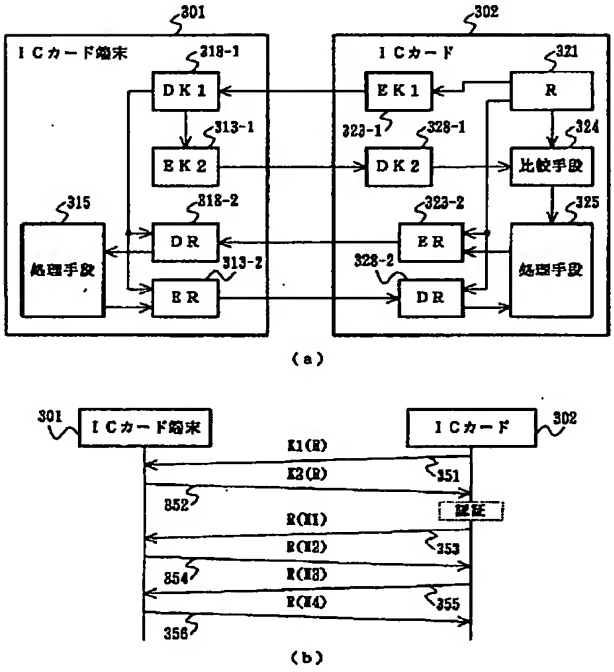
【図７】


401
ＩＣカード端末
412
Ｒ２
411
合成器
418-1
ＤＫ１
413-1
ＥＫ２
414
比較手段
418-2
ＤＫ３
415
処理手段
418-3
ＤＫ１Ｒ２
ＥＫ１Ｒ２
413-2
402
ＩＣカード
423-1
ＥＫ１
428-1
ＤＫ２
427
分離器
421
424
比較手段
423-2
ＥＫ３
423-3
ＥＫ１Ｒ２
425
処理手段
ＤＫ１Ｒ２
428-2
(a)
401
ＩＣカード端末
402
ＩＣカード
K1(R1)
K2(R1R2)
451
452
照合
K3(R2)
照合
453
K1R2(N1)
K1R2(N2)
454
455
K1R2(N3)
K1R2(N4)
456
457
(b)

【図８】


501
ＩＣカード端末
518-1
ＤＫ１
513-1
ＥＫ２
511
Ｒ２
531-1
レジスタ
515
処理手段
518-2
ＤＲ２
532-1
ＥＲ２
513-2
532-2
レジスタ
531-2
502
ＩＣカード
523-1
ＥＫ１
528-1
ＤＫ２
521
Ｒ１
541-1
レジスタ
542-1
523-2
ＥＲ２
525
処理手段
542-2
528-2
ＤＲ２
レジスタ
541-2
(a)
501
ＩＣカード端末
502
ＩＣカード
K1(R1)
K1(R2)
551
552
K2(N1) XOR R1
553
554
K2(N3) XOR R1
K2(N4) XOR R2
555
556
K2(N5) XOR R3
K2(N6) XOR R4
557
558
(b)

【図６】



フロントページの続き

(51)Int.Cl.[6]	識別記号	ＦＩ	
		Ｈ０４Ｌ　9/00	６７３Ｅ